On the Detection of Multi-Channel Man-in-the-Middle Attacks Aganist Wi-fi Networks

By Manesh Thankappan

Doctoral Thesis

Supervisors: Dr. Helena Rifà-Pous & Dr. Carles Garrigues Olivella

PhD THESIS IN NETWORK & INFORMATION TECHNOLOGIES

Universitat Oberta de Catalunya

Universitat Oberta de Catalunya

Doctoral Thesis

On the Detection of Multi-Channel Man-in-the-Middle Attacks Aganist Wi-fi Networks

Author:
Manesh Thankappan

Supervisors:
Dr. Helena Rifà-Pous
Dr. Carles Garrigues Olivella

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the
Doctoral Program in Network and Information Technologies

2018-2024

"A DREAM IS NOT THAT WHICH YOU SEE WHILE SLEEPING, IT IS SOMETHING THAT DOES NOT LET YOU SLEEP"

A.P.J. Abdul Kalam

TO MY DEAR FAMILY

For their prayers, unconditional love, and endless encouragement

Declaration of Authorship

I, Manesh Thankappan, hereby declare that I am the sole author of this thesis titled "On the Detection of Multi-Channel Man-in-the-Middle Attacks Against Wi-Fi Networks" and that the work presented herein is entirely my own. I affirm that this work was conducted in fulfillment of the requirements for the Doctoral degree in NETWORK & INFORMATION TECHNOLOGIES at the Universitat Oberta de Catalunya, Barcelona. All the sources used and cited have been properly acknowledged and listed in the reference section. No part of this thesis has been previously submitted for any degree or examination in any other university. This thesis is a result of my own work and includes nothing which is the outcome of work done in collaboration, except where specifically indicated in the text.

Manesh Thankappan

Digitally Signed
Signed by: Thankappan manesh
Reason: Signing the thesis
Location: Cochin,Kerala,India
Date: 16-May-2024 21:09:09

Date: May 2024

Certificate from Supervisors

The thesis supervisors declare that this thesis has been conducted in accordance with the guidelines and requirements for the format of a collection of contributions. The contributions presented herein are aligned with the thesis's proposed objectives and maintain thematic unity. Each article included in this compendium reflects a thorough examination of the research topic, showcasing originality and scholarly rigour. The impact factor and categorization of the journals publishing these articles further validate the significance and quality of the research. Therefore, the thesis supervisors approve the presentation of the thesis in this format.

Helena Rifà-Pous

Digitally signed by RIFA POUS HELENA - 77115233M
Date: 2024.05.15 23:46:01 +02'00'

Carles Garrigues Olivella

Firmado digitalmente por CARLOS GARRIGUES OLIVELLA el día 2024/05/16 a las 09:57:48 CEST

Date: May 2024

Abstract

Wireless networks face numerous security challenges, among which Man-in-the-Middle (MitM) attacks pose a significant threat. The Multi-Channel MitM (MC-MitM) attack, an advanced form of MitM, exploits wireless communications between clients and Access Points (APs) without needing legitimate Wi-Fi passphrases. This attack can be carried out on both personal and enterprise networks, regardless of the Wi-Fi encryption standard used. It involves cloning the legitimate AP on a different channel, enabling the attacker to intercept, manipulate, and relay communication between the client and AP. This doesn't break encryption but allows leveraging Wi-Fi standard flaws to capture or alter sensitive data. Some WPA-TKIP decryption attacks in 2014, wireless packet size exposing attacks in 2016, cipher downgrade attacks in 2017, key reinstallation attacks (KRACK) in 2017-18, and the latest FragAttacks in 2021 are frontline MC-MitM attacks. Among these attacks, KRACK and FragAttacks widely impacted millions of Wi-Fi systems, especially those with Internet of Things (IoT) devices, as they exploited certain programming mistakes of the Wi-Fi standard.

In the first part of the thesis, we evaluate MC-MitM attacks' capabilities in manipulating encrypted Wi-Fi communications, classifying them based on the attackers' objectives, and studying their impact. We extensively review existing defense mechanisms in confronting MC-MitM attacks, including a feasibility analysis. Existing defenses against MC-MitM attacks are often impractical, requiring firmware modifications or advanced hardware and software. On top of that, high technical overhead is imposed on users in terms of network setup and maintenance. We also enumerate several research problems regarding design deficiencies in confronting MC-MitM attacks in the standards. Based on these findings, our analysis indicates that an effective and easily deployable defense against MC-MitM threats within existing systems would be a signature-based detection system tailored for this type of attacks.

In the second part of the thesis, we first classify and empirically analyze the specific attack traffic during various MC-MitM attacks, comparing it with benign traffic. We then design lightweight attack signatures capable of passively and quickly identifying various MC-MitM attacks.

In the third part of the thesis we propose the SWIDS framework, the first of its kind to detect MC-MitM attacks. We design a plug-and-play monitoring system that can passively detect various MC-MitM attacks through specific signatures we have designed for this purpose. Our detection system can be easily integrated into any Wi-Fi or IoT environment, such as smart homes. We develop a prototype of the proposed framework using the python-scapy library. This system, evaluated in a smart home network, detected attacks within 60 seconds and an accuracy of more than 90% using detectors located at

a short distance from the attacker, and the accuracy was 84% using detectors at a long distance and under normal conditions. We also identify that frame loss affects detection performance, especially with detectors located at long distances.

In the last part of the thesis, we enhance our SWIDS by integrating a distributed and cooperative detection mechanism (DC-SWIDS), transforming it into several autonomous detection systems (ADS) that independently monitor and respond to MC-MitM threats. Utilizing MQTT for ADS node intercommunication, we implement DC-SWIDS on Raspberry Pis, allowing monitoring across multiple APs and channels. This distributed approach significantly reduces frame loss and improves the True Positive Rate (TPR) in detecting MC-MitM attacks. Evaluations in smart home settings show that DC-SWIDS achieves a TPR above 98% in detecting attacks when nodes are deployed in multiple locations in the testbed.

Overall, this research contributes to better understanding and improving the security against MC-MitM attacks, proposing practical intrusion detection solutions adaptable to various wireless environments, especially IoT, where security is paramount yet challenging to maintain.

Resumen

Las redes inalámbricas se enfrentan a numerosos desafíos de seguridad, entre los cuales los ataques Man-in-the-Middle (MitM) que representan una amenaza importante. El ataque Multi-Channel MitM (MC-MitM) es una forma avanzada de MitM que permite explotar las comunicaciones inalámbricas entre clientes y puntos de acceso (AP) sin necesidad de conocer las contraseñas de las Wi-Fi legítimas. Este ataque se puede llevar a cabo tanto en redes personales como empresariales independientemente del estándar de cifrado Wi-Fi utilizado. Consiste en clonar el AP legítimo en un canal diferente de forma que el cliente se conecte al AP falso y el atacante pueda interceptar, manipular y retransmitir la comunicación entre el cliente y el AP real. El ataque no busca romper el cifrado Wi-Fi sino aprovechar los fallos del estándar para capturar o alterar datos confidenciales. Algunos ataques de descifrado WPA-TKIP en 2014, ataques de exposición de tamaño de paquetes inalámbricos en 2016, ataques de degradación de cifrado en 2017, ataques de reinstalación de claves (KRACK) en 2017-18 y los últimos FragAttacks en 2021, son ejemplos de ataques conocidos que usan el modelo MC-MitM. Entre estos ataques, los más destacados son los KRACK y FragAttacks que impactaron a millones de sistemas Wi-Fi, especialmente aquellos con dispositivos de Internet de las cosas (IoT), ya que explotan ciertos errores de programación del estándar de comunicación inalámbrica.

En la primera parte de la tesis, evaluamos las capacidades de los ataques MC-MitM para manipular comunicaciones Wi-Fi cifradas, los clasificamos en función de los objetivos de los atacantes y estudiamos su impacto. Revisamos ampliamente los mecanismos de defensa existentes para hacer frente a los ataques MC-MitM, incluyendo un análisis de viabilidad. Las defensas existentes contra los ataques MC-MitM suelen ser poco prácticas ya que requieren modificaciones avanzadas del firmware o del hardware y el software. Además, conllevan una sobrecarga técnica elevada para los usuarios en términos de configuración y mantenimiento de la red. También enumeramos varios problemas de investigación relativos a las deficiencias de diseño de los estándares para hacer frente a los ataques MC-MitM. A partir de estos hallazgos, nuestro análisis indica que una defensa contra los ataques MC-MitM eficaz y senzilla de desplegar en los sistemas existentes sería un sistema de detección de intrusiones basado en firmas (SWIDS) diseñado para entornos de red diversos y dinámicos.

En la segunda parte de la tesis, primero clasificamos y analizamos empíricamente el tráfico generado a través de varios ataques MC-MitM y lo comparamos con el tráfico benigno. A continuación, diseñamos firmas de ataque ligeras que sean capaces de identificar pasiva y rápidamente diversos ataques MC-MitM.

En la tercera parte de la tesis proponemos el esquema SWIDS, el primero de su tipo para detectar ataques MC-MitM. Diseñamos un sistema de monitorización en línea plug-and-

play que puede detectar pasivamente diversos ataques MC-MitM a través de firmas específicas que hemos diseñado para este fin. Nuestro sistema de detección puede integrarse fácilmente en cualquier entorno Wi-Fi o IoT, como los hogares inteligentes. Desarrollamos un prototipo del esquema propuesto utilizando la librería python-scapy. Este sistema, evaluado en una red doméstica inteligente, es capaz de detectar ataques en menos de 60 segundos y una precisión de más del 90% utilizando detectores situados a poca distancia del atancante, y la precisión es del 84% usando detectores a larga distancia y en condiciones normales. También identificamos que la pérdida de tramas afecta el rendimiento de la detección, especialmente con detectores situados a larga distancia.

En la última parte de la tesis, mejoramos nuestro esquema SWIDS integrando un mecanismo de detección distribuido y cooperativo (DC-SWIDS) y transformándolo en varios sistemas de detección autónomos (ADS) que monitorizan y responden de forma independiente a las amenazas MC-MitM. Utilizando MQTT para la intercomunicación de nodos ADS, implementamos DC-SWIDS en Raspberry Pis, lo que permite el monitoreo a través de múltiples AP y canales. Este enfoque distribuido reduce significativamente la pérdida de tramas y mejora la tasa de verdaderos positivos (TPR) en la detección de ataques MC-MitM. Las evaluaciones en entornos de hogares inteligentes muestran que el esquema DC-SWIDS logra una taza de detección de ataques superior al 98% cuando se despliegan los nodos en varias ubicaciones del entorno de pruebas.

En general, esta investigación contribuye a comprender mejor y mejorar la seguridad contra los ataques MC-MitM, proponiendo soluciones prácticas de detección de intrusiones adaptables a diversos entornos inalámbricos, especialmente IoT, donde la seguridad es primordial pero difícil de mantener.

Resum

Les xarxes sense fil s'enfronten a nombrosos reptes de seguretat, entre els quals els atacs Man-in-the-Middle (MitM) que representen una amenaça important. L'atac MitM multi-canal (MC-MitM) és una forma avançada de MitM que permet explotar les comunicacions sense fils entre clients i punts d'accés (AP) sense necessitat de conèixer les contrasenyes de les Wi-Fi legítimes. Aquest atac es pot dur a terme tant en xarxes personals com empresarials independentment de l'estàndard de xifrat Wi-Fi utilitzat. Consisteix a clonar l'AP legítim en un canal diferent de manera que el client es connecti a l'AP fals i l'atacant pugui interceptar, manipular i retransmetre la comunicació entre el client i l'AP real. L'atac no busca trencar el xifrat Wi-Fi sinó aprofitar les fallades de l'estàndard per a capturar o alterar dades confidencials. Alguns atacs de desxifrat WPA-TKIP el 2014, atacs d'exposició de grandària de paquets sense fils el 2016, atacs de degradació de xifrat el 2017, atacs de reinstal·lació de claus (KRACK) el 2017-18 i els últims FragAttacks el 2021, són exemples d'atacs coneguts que usen el model MC-MitM. Entre aquests atacs, els més destacats són els KRACK i FragAttacks que van impactar a milions de sistemes Wi-Fi, especialment aquells amb dispositius d'Internet de les coses (IoT), ja que exploten certs errors de programació de l'estàndard de comunicació sense fil.

A la primera part de la tesi, avaluem les capacitats dels atacs MC-MitM per a manipular comunicacions Wi-Fi xifrades, els classifiquem en funció dels objectius dels atacants i estudiem el seu impacte. Revisem àmpliament els mecanismes de defensa existents per a fer front als atacs MC-MitM, incloent una anàlisi de viabilitat. Les defenses existents contra els atacs MC-MitM solen ser poc pràctiques ja que requereixen modificacions avançades del firmware o del maquinari i el programari. A més, comporten una sobrecàrrega tècnica elevada per als usuaris en termes de configuració i manteniment de la xarxa. També enumerem diversos problemes de recerca relatius a les deficiències de disseny dels estàndards per a fer front als atacs MC-MitM. A partir d'aquestes troballes, la nostra anàlisi indica que una defensa contra els atacs MC-MitM eficaç i senzilla de desplegar en els sistemes existents seria un sistema de detecció d'intrusions basat en signatures (SWIDS) dissenyat per a entorns de xarxa diversos i dinàmics.

A la segona part de la tesi, primer classifiquem i analitzem empíricament el trànsit generat a través de diversos atacs MC-MitM i el comparem amb el trànsit benigne. A continuació, dissenyem signatures d'atac lleugeres que siguin capaces d'identificar passiva i ràpidament diversos atacs MC-MitM.

A la tercera part de la tesi proposem l'esquema SWIDS, el primer del seu tipus per a detectar atacs MC-MitM. Dissenyem un sistema de monitoratge en línia plug-and-play que pot detectar passivament diversos atacs MC-MitM a través de signatures específiques que hem dissenyat per a aquesta fi. El nostre sistema de detecció pot integrar-se fàcilment

en qualsevol entorn Wi-Fi o IoT, com les llars intel·ligents. Desenvolupem un prototip de l'esquema proposat utilitzant la llibreria python-scapy. Aquest sistema, avaluat en una xarxa domèstica intel·ligent, és capaç de detectar atacs en menys de 60 segons i una precisió de més del 90% utilitzant detectors situats a poca distància de l'atancant, i la precisió és del 84% usant detectors a llarga distància i en condicions normals. També identifiquem que la pèrdua de trames afecta el rendiment de la detecció, especialment amb detectors situats a llarga distància.

A l'última part de la tesi, millorem el nostre esquema SWIDS integrant un mecanisme de detecció distribuït i cooperatiu (DC-SWIDS) i transformant-ho en diversos sistemes de detecció autònoms (ADS) que monitoritzen i responen de manera independent a les amenaces MC-MitM. Utilitzant MQTT per a la intercomunicació de nodes ADS, implementem DC-SWIDS en Raspberry Pis, la qual cosa permet el monitoratge a través de múltiples AP i canals. Aquest enfocament distribuït redueix significativament la pèrdua de trames i millora la taxa de veritables positius (TPR) en la detecció d'atacs MC-MitM. Les avaluacions en entorns de llars intel·ligents mostren que l'esquema DC-SWIDS aconsegueix una tassa de detecció d'atacs superior al 98% quan es despleguen els nodes en diverses ubicacions de l'entorn de proves.

En general, aquesta recerca contribueix a compendre i millorar la seguretat contra els atacs MC-MitM, proposant solucions pràctiques de detecció d'intrusions adaptables a diversos entorns sense fils, especialment IoT, on la seguretat és primordial però difícil de mantenir.

Acknowledgemnents

During my tenure at the Universitat Oberta de Catalunya (UOC), I have had the opportunity to work with distinguished professors and fellow researchers who have made my doctoral research experience into one I will cherish for the rest of my life. This section is intended to express my heartfelt gratitude to those who provided me with support and assistance during my PhD research and during the preparation of this thesis.

First and foremost, I extend my deepest gratitude to my supervisors, Dr. Helena Rifà-Pous and Dr. Carles Garrigues, for their invaluable guidance, steadfast support, and constant motivation. I am immensely thankful for your insightful advice and suggestions, which were crucial in navigating the challenges encountered during my research. Your wise counsel has been tremendously inspirational and instrumental in enhancing the quality of my research, my publications, and my thesis.

I am also grateful to Professor David Megias and all the distinguished faculty members and researchers of the KISON group. Your astute comments during our research meetings have been invaluable to my work. Additionally, I thank both the UOC and the KISON group for providing research funding and the essential computing resources needed for conducting my Wi-Fi experiments.

Special thanks go to Dr. Mathy Vanhoef, the originator of the MC-MitM attack, for sharing your source codes and assisting me with resolving numerous critical issues throughout my research and experimentation. Working with your groundbreaking research papers has been a profoundly enlightening and inspiring experience, broadening my understanding of wireless security challenges.

My sincere appreciation extends to the Fundació per a la Universitat Oberta de Catalunya (FUOC) for awarding me a PhD fellowship and additional research funding. I also wish to acknowledge the support from the Spanish Ministry of Economy and Competitiveness under Grant RTI2018-095094-B-C22 "CONSENT", and under Grant PID2021-125962OB-C31 “SECURING". I also sincerely acknowledge the funding support from Ministerio de Ciencia e Innovación, la Agencia Estatal de Investigación and the European Regional Development Fund (ERDF) under Project PID2021-125962OB-C31; and the ARTEMISA International Chair of Cybersecurity and the DANGER Strategic Project of Cybersecurity, the Spanish National Institute of Cybersecurity through the European Union-NextGenerationEU and the Recovery, Transformation and Resilience Plan.

Thank you to everyone in the Human Resources and Administration departments, especially Nuria Garcia Palma, Trina Garcia-Parra López-Acosta, and Carolina Campalans Moncada, for your assistance and for meticulously maintaining my documentation during my tenure at UOC.

I am also thankful for the team managing the computer infrastructure at UOC. Your efforts in providing computers configured to my specifications have been essential for my advanced experiments on Linux.

To my fellow PhD researchers, particularly Dr. Hassan Hayat, your camaraderie and stimulating discussions have made this journey enjoyable and enriching. A heartfelt thanks to my dear friend Jamil Ahmadkassem for his support during my experiments and research.

Last but certainly not least, my deepest gratitude goes to my family. To my beloved parents, Thankappan and Laly, to my wife, Lekha, and to my cherished children, Lakshna and Milasha, your love, prayers, and unwavering support have been my greatest strength. Thank you for your continuous encouragement and for believing in me.

In closing, I am indebted to all my teachers and mentors whom I've had the honor of learning from throughout my life. I humbly acknowledge your enduring support. Finally, I extend my sincere thanks to all my colleagues and friends from the UOC community. The past five years have been an intensely educative and personally enriching experience. Without your collective support, completing this thesis would not have been possible.

Manesh Thankappan

List of Acronyms

Acronym	Definition
ADS	**A**utonomous **D**etection **S**ystem.
AES	**A**dvanced **E**ncryption **S**tandard.
AP	**A**ccess **P**oint.
ARP	**A**ddress **R**esolution **P**rotocol.
BIGTK	**B**eacon **I**ntegrity **G**roup **T**emporal **K**ey.
BIP	**B**roadcast **I**ntegrity **P**rotocol.
BSS	**B**asic **S**ervice **S**et.
BSSID	**B**asic **S**ervice **S**et **I**dentifier.
CBC	**C**ipher **B**lock **C**haining.
CBTC	**C**ommunication **B**ased **T**rain **C**ontrol.
CCMP	**C**ounter Mode with **C**ipher Block Chaining **M**essage **P**rotocol.
CERT	**C**omputer **E**mergency **R**esponse **T**eam
CMAC	**C**lient **M**edium **A**ccess **C**ontrol.
CRC	**C**yclic **R**edundancy **C**ode.
CRP	**C**hallenge **R**esponse **P**air.
CSA	**C**hannel **S**witch **A**nnouncement.
CSMA/CD	**C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance.
CVE	**C**ommon **V**ulnerabilities and **E**xposures.
DC-SWIDS	**D**istributed and **C**ooperative **S**ignature-Based **W**ireless **I**ntrusion **D**etection **S**ystem
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol.
DNS	**D**omain **N**ame **S**ystem.
DOS	**D**enial **o**f **S**ervice.
EAPOL	**E**xtensible **A**uthentication **P**rotocol **O**ver **L**AN.
ECC	**E**lliptic **C**urve **C**ryptography.
ECDH	**E**lliptic **C**urve **D**iffie **H**elman.
FCS	**F**rame **C**heck **S**equence.
GCMP	**G**alois **C**ounter **M**ode **P**rotection.
GTK	**G**roup **T**emporal **K**ey.
GUI	**G**raphical **U**ser **I**nterface
HTTP	**H**yper**t**ext **T**ransfer **P**rotocol.
HSTS	**H**TTP **S**trict **T**ransport **S**ecurity.
HTTPS	**H**yper**t**ext **T**ransfer **P**rotocol Secure.
ICV	**I**ntegrity **C**heck **V**alue.
IDS	**I**ntrusion **D**etection **S**ystem.
IE	**I**nformation **E**lement.
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers.

IGTK	**I**ntegrity **G**roup **T**emporal **K**ey.
IP	**I**nternet **P**rotocol.
IV	**I**nitialization **V**ector.
KRACK	**K**ey **R**einstallation **A**tta**ck**.
LAN	**L**ocal **A**rea **N**etwork.
MAC	**M**edium **A**ccess **C**ontrol.
MitM	**M**an-**i**n-**t**he-**M**iddle.
MC-MitM	**M**ulti-**C**hannel **M**an-**i**n-**t**he-**M**iddle.
MIC	Message Integrity Code.
MME	**M**essage **I**ntegrity **C**ode **E**lement.
MQTT	**M**essage **Q**ueuing **T**elemetry **T**ransport
NIC	**N**etwork **I**nterface **C**ard.
OCI	**O**perating **C**hannel **I**nformation.
OCV	**O**perating **C**hannel **V**alidation.
OS	**O**perating **S**ystem.
PK	**P**ublic **K**ey.
PMF	**P**rotected **M**anagement **F**rame.
PMK	**P**re-**M**aster **K**ey.
PRF	**P**seudo **R**andom **F**unction.
PSK	Pre-Shared Key.
PTK	**P**airwise **T**ransient **K**ey.
PWE	**P**assword **E**lement.
RC4	**R**ivest **C**ipher 4.
RNG	**R**andom **N**umber **G**enerator.
RSN	**R**obust **S**ecurity **N**etwork.
RSNE	**R**obust **S**ecurity **N**etwork **E**lement.
RSSI	**R**eceived **S**ignal **S**trength **I**ndicator.
SA	**S**ecurity **A**ssociation.
SAE	**S**imultaneous **A**uthentication of **E**quals.
SSID	**S**ervice **S**et **I**dentifier.
SWIDS	**S**ignature-Based **W**ireless **I**ntrusion **D**etection **S**ystem
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol.
TLS	**T**ransport **L**ayer **S**ecurity.
TPK	**T**unneled Link **P**eer **K**ey.
URL	**U**niform **R**esource **L**ocator
WEP	**W**ired **E**quivalent **P**rivacy.
WFA	**W**i-**F**i **A**lliance.
Wi-Fi	**Wi**reless **Fi**delity
WIDS	**W**ireless **I**ntrusion **D**etection **S**ystem
WLAN	**W**ireless **LAN**.
WNM	**W**ireless **N**etwork **M**anagement.
WPA	**W**i-Fi **P**rotected **A**ccess.
WPA2	**W**i-Fi **P**rotected **A**ccess Version **2**.
WPA3	**W**i-Fi **P**rotected **A**ccess Version **3**.

CONTENTS

1

General Introduction

Chapter 1

General Introduction

Wireless networks are increasingly prevalent in many networking contexts due to the flexibility, mobility, and ease of access they provide. This popularity is further bolstered by the integration of Internet of Things (IoT) devices, which frequently utilize the 802.11 standards. Despite their advantages, WLANs are vulnerable to a variety of wireless security threats, including Man-in-the-Middle (MitM) attacks. Such attacks pose a significant risk to wireless networks by enabling attackers to intercept and manipulate communications between two endpoints. In a typical MitM attack, the attacker is strategically positioned between the client and the Access Point (AP), in order to perform other attacks from this position that could allow them to eavesdrop, alter messages, and even impersonate one of the communicating parties. In the simplest form of such attacks, the attacker introduces a laptop with two Wi-Fi cards; one of them is connected to the legitimate AP or his own AP, and the other acts as a rogue AP (also known as an evil-twin), spoofing the legitimate AP so that clients will connect to it because of the commonly used automatic AP selection option [1]. In general, there are two approaches to perform MitM attacks in a WLAN.

1. In the traditional approach to rogue AP MitM attacks, the attacker establishes a new rogue AP. What is important in this case is that the attacker knows the network shared key or passphrase. The rogue AP broadcasts the same SSID (Service Set Identifier) or network name as the legitimate network. Unsuspecting users, thinking they are connecting to a trusted network, connect to the rogue AP instead. Once a user connects to the rogue network, the attacker can monitor all the user's traffic. This can include the interception of sensitive data such as passwords and other personal information (if the application protocol does not include encryption). For example, attackers can redirect users to a fake authentication web page to deceive users and fetch legitimate website passwords. Therefore, traditional rogue AP MitM attacks require a known Wi-Fi passphrase for manipulating encrypted traffic between the client and the AP. Additionally, these attacks largely rely on user actions, such as connecting to a rogue network. Common tools used for these types

of attacks include Fluxion [2], Wifiphisher [3], WiFi-Pumpkin [4], and Airbase-ng [5].

2. In 2014, Vanhoef and Piessens [6] introduced a more advanced MitM approach known as Multi-Channel MitM (MC-MitM) attack. This advanced approach involves the attacker using a laptop equipped with two Wi-Fi cards, each operating on a different channel. Specifically, one Wi-Fi card clones the legitimate AP on an alternative or rogue channel for the clients (victims) to connect to, while the other card impersonates the client on the legitimate channel to maintain a connection with the legitimate AP. Such a configuration facilitates the attacker exchanging all connection establishment and data frames between both channels so that they can communicate with both the client and the AP simultaneously [6], [7]. This setup allows the attacker to place herself in the MitM position, between the client and the legitimate AP, without the need for legitimate Wi-Fi passphrases. Furthermore, such an approach of frame exchange is effective regardless of the client's authentication method, making MC-MitM attacks viable in both personal and enterprise Wi-Fi networks. Once the MC-MitM position is acquired, the attacker can use other attacks to block and modify encrypted frames between the client and legitimate AP. It is important to note that the MC-MitM position does not break any encryption, but it is primarily used as the initial step needed to perform further attacks that exploit specific weaknesses (e.g., flaws in authentication or encryption) in Wi-Fi standards such as WPA, WPA2, or WPA3. Such attacks exploit vulnerabilities in Wi-Fi protocols that can result in a denial of service (DoS), security downgrades, and key reinstallations (KRACK), as well as newer attacks like FragAttacks. This advanced approach highlights a significant evolution in the tactics used in MitM attacks. We also emphasize that MC-MitM attacks are significantly more potent if the Wi-Fi passphrase is known. Attackers can then decrypt, modify, and re-encrypt Wi-Fi communication frames (irrespective of exploiting any vulnerabilities) between the victim and the legitimate AP in real-time, allowing for direct and serious manipulations as demonstrated by Chi et al. [8]. In contrast, traditional rogue AP attacks mostly capture wireless communication for offline decryption (using a known passphrase) and attempts to extract personal data, lacking the capability for on-the-fly manipulation between the victim and the AP.

This thesis is focused on the advances of MC-MitM attacks. Essentially, to establish an MC-MitM position, attackers utilize either jamming techniques or channel switch announcements (CSAs) to compel clients to switch to controlled channels. This thesis distinguishes between two types of MC-MitM attacks. Those using jamming are categorized as **MC-MitM base variant attacks** (MC-MitM-BV), while those employing CSAs are termed **MC-MitM improved variant attacks** (MC-MitM-IV).

1.1 Frontline MC-MitM attacks

The most prominent and well-known example of attack that uses a MC-MitM-BV in its initial stage is the key reinstallation attack (KRACK). Introduced by Vanhoef et al. in October 2017 [9], KRACK targeted critical vulnerabilities in the nonce reuse process during the 4-way handshake of the IEEE 802.11 standards. These vulnerabilities allow attackers to decrypt Wi-Fi frames, predominantly affecting Linux and Android devices, as these platforms were prone to use an all-zero encryption key in response to key reinstallation attacks under WPA or WPA2 protocols. This landmark discovery marked the first non-vendor-specific vulnerability, impacting millions of devices globally due to flawed implementation of the standard.

FragAttacks, released by Vanhoef et al. in May 2021 [10], are the latest set of non-vendor-specific and most impactful attacks performed using the MC-MitM improved variants. With FragAttacks, the attacker exploits a set of authentication weaknesses in the aggregation and fragmentation feature of IEEE 802.11 standards by injecting packets into encrypted Wi-Fi networks for tricking the client into using a malicious web server and obtaining sensitive client information. These MC-MitM attacks also affect the WPA3 standard. Like KRACK, there are also millions of Wi-Fi devices that are vulnerable to FragAttacks due to faulty implementation of the standard or flaws in the Wi-Fi algorithms.

MC-MitM attacks have been exploited in some critical systems. For instance, research conducted by Chi et al. [8] demonstrated that an improved variant of the MC-MitM attack could be used to disrupt train control systems by inducing emergency braking and system failure. In this scenario, the attacker employs the MC-MitM position to capture Wi-Fi frames (train control messages) between two legitimate devices and decrypts them on-the-fly using tools like the pyDot11 open-source library. This attack illustrates that MC-MitM attackers are more powerful when they are insiders or possess the Wi-Fi passphrase.

1.2 Challenges in detecting MC-MitM attacks

Following the disclosure of the significant key reinstallation vulnerability (KRACK), the Wi-Fi Alliance (WFA) and prominent Wi-Fi chip manufacturers became increasingly aware of KRACK attacks. In response, patches were developed and released to address these vulnerabilities. However, these patches are predominantly effective only on the more sophisticated Wi-Fi clients such as laptops, smartphones, and routers. The patching of many other devices is often not feasible, especially for IoT devices, which may not be supported by their manufacturers or may lack the necessary network settings for the updates. As a result, a vast number of devices operating on WPA or WPA2 standards, particularly within the IoT spectrum, remain vulnerable to these attacks driven by the

MitM position.

Several leading device manufacturers (e.g., Google [11], Aruba [12], Cisco [13]) studied the severity level and impact of key reinstallation vulnerabilities on their products. They also issued security patches for impacted devices and recommended several configuration adjustments to help mitigate these attacks. However, a significant issue remains as many vendors fail to release patches even when notified by responsible authorities. According to the CERT (Computer Emergency Response Team) data 2017 [14], only 17% of notified vendors released KRACK patches during the coordinated patch release period. An exploratory study in August 2020 [15] highlighted that about 65% of tested Wi-Fi and IoT devices were vulnerable. The emergence of FragAttacks, which exploit Wi-Fi aggregation and fragmentation vulnerabilities, has exacerbated concerns about the security of IoT devices, which seldom receive updates and are thus prone to the same patching challenges seen with earlier KRACK attacks. While patches for MC-MitM attacks like KRACK and FragAttacks exist for WPA2 and WPA3 devices, WPA devices remain unprotected against several critical vulnerabilities, TKIP group cipher attacks [9], TKIP downgrade and group key recover attacks [16], wireless packet size exposing attacks [17]. This lack of security updates is due to the Wi-Fi Alliance's deprecation of the TKIP protocol [18].

In addition to deploying patches, the WFA mandated the implementation of the 802.11w standard, also known as Protected Management Frames (PMF) [19], to safeguard wireless communications from spoofed deauthentication or disassociation attacks that are typical in MitM or DoS scenarios. Despite these measures, PMF remains insufficient in combating MC-MitM attacks for several reasons. First, MC-MitM attackers do not rely on deauthentication packets to establish their position within the network [20]; second, PMF does not have the capability to detect jamming attacks [21]; and third, MC-MitM attacks often utilize beacons or probe responses, which are not covered by PMF protections [22].

Once the MC-MitM position is secured, the attacker has the opportunity to launch a variety of attacks, exploiting vulnerabilities within the PMF standard itself. These attackers can also engage in sophisticated tactics such as channel switch attacks [23], jamming legitimate channel switch announcements [24], and forging reassociation frames, leading to potential network deadlock or Denial of Service (DoS) [25]. The ability to execute these attacks often requires only a single forged frame, making them particularly difficult to detect in real-world conditions.

Detecting MC-MitM attacks is challenging due to the intrinsic nature of the tactics employed by attackers, who mimic the characteristics of both the legitimate AP and the client. In this regard, MC-MitM attackers can fine-tune the transmission power and other discernible features to blend seamlessly into the network environment [26].

Moreover, the utilization of CSA frames allows attackers to redirect clients to rogue APs [24], [27]. This capability significantly complicates prevention efforts and remains a per-

sistent vulnerability across all Wi-Fi Protected Access (WPA) standards, including the newer WPA3. Given these factors, relying solely on RSSI-based detection proves inadequate in identifying and thwarting MC-MitM attacks.

To establish a MitM position, the MC-MitM attacker may deploy techniques such as reactive jamming using affordable, readily available Wi-Fi adapters. These methods are particularly challenging for intrusion detection systems to detect because the attack generates random noise pulses. These pulses can easily be mistaken for interference from non-Wi-Fi devices operating on similar frequency bands, complicating the task of distinguishing malicious activities from ordinary network behaviors [6], [28]. This complexity underscores the need for more sophisticated detection strategies that can differentiate between typical behavior of wireless network actions and malicious interventions.

Traditional perimeter security measures such as firewalls and VPNs are commonly implemented to safeguard network communications. Nonetheless, these measures are largely ineffective against MC-MitM attacks, which operate at the link layer, while firewalls and VPNs address vulnerabilities at higher layers of the network stack. In addition, while SNORT [29] provides rules that can identify network packets containing specific elements associated with KRACK attack tools or scripts, such as Dot11, RadioTap, or FCfield, these rules may fail to detect variations of these attacks. This is because the packet contents identified by SNORT may also appear in legitimate WLAN traffic, potentially leading to false alarms or ineffectiveness in real-world scenarios. Furthermore, SNORT detects KRACK attacks after the MitM position is acquired. It cannot detect the first stage of the attack, where the MC-MitM vulnerability is exploited.

Despite the existence of testing frameworks [30] that can identify vulnerabilities related to fragmentation and aggregation in Wi-Fi devices, specialized defense mechanisms to protect against FragAttacks are still lacking. This highlights a significant gap in current security protocols that needs to be addressed to enhance protection against these advanced types of cybersecurity threats.

To counteract the strategies employed by MC-MitM attackers, the WFA implemented enhancements to the IEEE 802.11 standards in 2020. These enhancements include the introduction of Operating Channel Validation (OCV) [22], which serves as a direct preventive mechanism against MC-MitM attacks. Additionally, the WFA incorporated Beacon Protection [31], a defense mechanism designed to thwart the spoofing of beacon frames, a common tactic in MC-MitM attacks that exploit unauthenticated CSAs. Nonetheless, these measures require that all devices support the patched PMF standards, leaving the door open for certain types of partial MitM attacks. Additionally, the WFA implemented the Simultaneous Authentication of Equals-Public Key (SAE-PK) [32] as part of WPA3 standards, especially to secure public Wi-Fi against rogue APs. The SAE-PK authenticates APs uniquely via the digital signature of their public key during connection establishment. However, this only identifies rogue APs during the initial connection phase

or during the SAE-PK authentication, which does not prevent an MC-MitM attacker from intervening in ongoing connections between clients and APs. In certain defense mechanisms [28], anomalies are detected based on the AP's identities, such as the SSID (network name) and BSSID (MAC address). However, implementing these mechanisms can be costlier due to the requirement for multiple firmware modifications on all devices.

1.3 Motivation

The landscape of cybersecurity within Wi-Fi networks is continuously evolving, particularly in networks that incorporate a diverse array of Internet of Things (IoT) devices. Notably, MC-MitM attacks present a formidable challenge due to their complexity and the severe implications they can have on wireless security. Currently, there is a significant gap in the literature concerning a comprehensive review and analysis of various MC-MitM attack strategies and their impacts. This gap underscores the critical need for robust defense mechanisms tailored to these advanced threats.

The issues related to patching and the inherent vulnerabilities within both WPA2 and WPA3 frameworks demonstrate the challenges in effectively safeguarding Wi-Fi networks against MC-MitM attacks. Particularly, IoT devices exhibit increased susceptibility due to their limited resources, which often preclude the use of security updating. These issues are exacerbated by the inadequacies of current security protocols to seamlessly protect against such threats, especially when attackers can circumvent PMF protection and employ tactics like jamming and creation of rogue APs.

Moreover, the recent defense mechanisms like the OCV [22], Beacon Protection [31], SAE-PK [32], and improved PMF standards have not been universally adopted by device manufacturers, leaving numerous devices vulnerable to MC-MitM attacks. A primary reason for this is that these methods are implemented as optional features within the 802.11 standards. Activating these features can lead to compatibility issues across newer and older devices in typical Wi-Fi networks. The reality that legacy and low-resource devices continue to populate our networks means that any effective security strategy must accommodate a wide range of device capabilities and defense requirements.

Therefore, there is a pressing need for innovative and practical solutions that address these vulnerabilities and to improve the security against MC-MitM attacks. The motivation for this thesis is to develop a wireless intrusion detection system (WIDS) that is not only effective against a broad spectrum of MC-MitM attacks but also adaptable to the diverse landscape of Wi-Fi-based IoT environments. This system should be generic, lightweight, and capable of integrating seamlessly into existing network infrastructures without necessitating changes in existing hardware or software devices. Such a system would ideally provide continuous protection, leveraging the intrinsic capabilities of IoT devices while mitigating the risks posed by these sophisticated cyber threats.

In summary, the persistent and evolving nature of MC-MitM threats, combined with the challenges posed by IoT device integration into Wi-Fi networks, highlights the necessity for a new solution to these attacks. This thesis aims to address these challenges by proposing a novel intrusion detection framework designed to robustly counteract MC-MitM attacks, thereby contributing to the security of WiFi networks.

1.4 Objectives of the thesis

This thesis aims to accomplish the following objectives:

- **O1. To review the state of the art of MC-MitM attacks.** In our background analysis, we focus on the security of protected Wi-Fi networks, particularly the security provided at the link layer by the WPA, WPA2, and WPA3 protocols of IEEE 802.11 standards. Our objective is to explore the fundamentals of MitM attacks in Wi-Fi networks and the security provisions of the PMF standard. We seek to examine different variants of MC-MitM attacks, identifying protocol vulnerabilities and assessing their security implications across various platforms. Lastly, we evaluate existing defense mechanisms, particularly in the IoT context, to determine their technical viability in countering MC-MitM attacks.

- **O2. To empirically analyze specific attack traffic during MC-MitM attacks and create potential attack signatures.** Our goal is to recreate various types of MC-MitM attacks and analyze network behavior during the attacks. We intend to compare this traffic with benign wireless traffic from WPA, WPA2 and WPA3 networks, including enterprise (university) and home settings. This analysis will help to design attack signatures to effectively distinguish abnormal traffic patterns during MC-MitM attacks.

- **O3. To design, develop and evaluate a signature-based wireless intrusion detection system framework that can be used in any Wi-Fi or IoT environment**. We aim to design a wireless intrusion detection system framework that facilitates passive monitoring of network traffic in order to detect the MC-MitM attack signatures. We plan to develop the proposed intrusion detection system using the Python-Scapy library, which is an interactive packet manipulation program. We want to test our proposed system in a practical Wi-Fi-based IoT environment, such as a smart home with a variety of devices that support different Wi-Fi standards. We also aim to compare our proposed system with other existing defense mechanisms or tools.

- **O4. To extend the signature-based wireless intrusion detection system framework to include a distributed and cooperative detection strategy.** We introduce a distributed intrusion detection methodology that will enhance the

detection performance of the system to ensure wider surveillance against MC-MitM attacks. Such distributed systems will then be implemented on single-board computers (Raspberry Pis) and evaluated in real-world Wi-Fi-based IoT environments.

1.5 Research methodology

The research presented in this thesis was conducted using three different research methodologies. The ***Literature Review*** research methodology entails organizing relevant academic papers to explore advancements in various MC-MitM attacks and their impacts and conduct an extensive and comprehensive state of the art review. This process helps identify research gaps, which then guide the subsequent investigations and experiments conducted in this thesis.

The ***Design and Creation*** research methodology focused on outlining the objectives and requirements of the system, followed by the design and implementation of (1) different attack signatures of MC-MitM attacks, (2) design and development of a signature-based wireless intrusion detection system (SWIDS) framework, (3) design and development of a distributed and cooperative SWIDS framework.

During the ***Experimentation phase***, the methodology involved the deployment of the developed system in a controlled environment. This deployment allowed for the testing and evaluation of the system's performance, functionality, and effectiveness. Feedback and data collected from these experiments were then analyzed to identify areas for improvement and optimization.

The methodology for ***Design and Creation***, as well as ***Experimentation***, involved an iterative application to improve and optimize the system. This iterative approach allowed for continual refinement and enhancement of the system's throughout its development lifecycle.

1.6 Main contributions of the thesis

This thesis provides multiple novel contributions towards detecting MC-MitM attacks, especially in the context of IoT environments.

- **C1. Conducting a state of the art literature review of MC-MitM attacks for Wi-Fi networks.** To the best of our knowledge, this is the first comprehensive review that extensively covers various MC-MitM attacks. This review helped us to come up with the following contributions:
  - **C1.1 An in-depth evaluation of capabilities of MC-MitM attacks in manipulating protected Wi-Fi communications, such as WPA,**

WPA2 and WPA3. In this evaluation, we conducted an in-depth analysis of protocol specifications of WPA, WPA2, and WPA3. We then analyzed the technical setup, inner working principles of MC-MitM attacks, and tactics to exploit protocol vulnerabilities to deceive victims. This evaluation helped us to classify MC-MitM attacks (attack variants). We also evaluated the working principles of KRACK and FragAttacks, which are the most impactful attacks launched using the MC-MitM setup. This evaluation helped us to learn how Wi-Fi communication could be decrypted using KRACK and how sensitive data could be accessed through FragAttacks without needing to know the pre-shared passphrase. A comparison was also made between capabilities of MC-MitM attacks and traditional rogue AP MitM attacks. We then congregated and analyzed every MC-MitM enabled attack launched by different attack variants reported in the literature so far. This impact analysis provided us insights into how MC-MitM attacks are crafted to exploit various vulnerabilities, applicability of attacks on PMF standards, various repercussions of such attacks, the devices or platforms impacted, and the availability of security patches for different vulnerabilities within the 802.11 standard.

– **C1.2 A technical feasibility analysis of existing defense mechanisms for MC-MitM attacks.** In this analysis, we identified several significant challenges in terms of availability and applicability of security patches, especially on IoT devices. We also identified several challenges in adopting the PMF standard among every Wi-Fi or IoT device, and found that this standard is not a deterrent against MC-MitM attacks as such attacks have many tactics to circumvent PMF standard. We also analyzed the possible impacts of MC-MitM attacks in WPA3 networks because of their ability to circumvent PMF protection by creating relevant attack scenarios. We then categorized and assessed various existing defense mechanisms, focusing on strategies employed before (stage 1 defense) and after (stage 2 defense) an attacker achieves an MC-MitM position. This review highlighted the strengths and weaknesses of existing defenses and assessed their technical feasibility, especially in IoT environments. Considerations included changes in wireless standards, the need for PMF, the need for firmware updates, and the necessity for third-party software and hardware, along with computational complexity and technical overhead. This analysis helped us to uncover multiple research gaps due to standard design deficiencies and the technical infeasibility issues of current security measures against MC-MitM attacks. We also noted significant research challenges such as insufficient backward compatibility and the ineffectiveness of traditional spoofing detection methods in deterring MC-MitM attacks. Based on these findings, our analysis suggests that an effective and easily deploy-

able defense against MC-MitM threats within existing systems would be a signature-based detection system tailored for this type of attack.

The above contributions address the objective **O1**. The results of the state-of-the-art analysis are published as a review article entitled **"Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review"** in the **Expert Systems with Applications Journal.** This publication forms **Chapter 2** of this thesis.

- **C2. Designing MC-MitM attack signatures.** For this contribution, we performed a comprehensive empirical analysis of the behaviors exhibited by various MC-MitM attack variants. Additionally, we developed a unique dataset that is the first of its kind.
  - **C2.1. Creation of MC-MitM attack signatures.** In order to detect MC-MitM attacks, we first defined the theoretical threshold values that should trigger the detection of the different attack variants. These threshold values were validated using an experimental testbed, where we analyzed the network attack traffic using Wireshark. From these thresholds, we determined the attack signatures needed for detection.
  - **C2.2. Creation of Dataset for MC-MitM attacks.** We created a dataset that illustrates network behavior under MC-MitM attacks by capturing wireless frames in a Wi-Fi network using the Wireshark software. We also interpreted this dataset in terms of various stages of MC-MitM attacks and provided appropriate Wireshark filters. This dataset was compiled from a series of MC-MitM attack simulations in a controlled environment and has been made publicly available to support further research in this field.

  The above contributions address the objective **O2** and the results of this contribution are published as a research article entitled **"Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks and their attack signatures"** in the **Springer International Conference on Computer, Communication, and Signal Processing 2023 (ICCCSP '23)**, Tamil Nadu, India. This publication forms **Chapter 3** of this thesis.

- **C3. Designing and developing a Signature-Based Wireless Intrusion Detection System (SWIDS) framework.** The aim of this contribution is to create a plug-and-play signature-based wireless intrusion detection system framework, which is first of its kind and can be used in any Wi-Fi network.
  - **C3.1 Designing of SWIDS framework.** For this contribution, we designed a signature-based wireless intrusion detection system that utilizes the previously designed attack signatures **(contribution C2.1)** to detect different MC-

MitM attacks. The core of this framework is a set of traffic analysis algorithms that identify the presence of MC-MitM attack frames using the aforementioned signatures. We employed a threshold-based detection methodology to quickly and accurately detect abrupt and highly deviating changes in the network traffic due to MC-MitM attacks.

  - **C3.2 Development of an open source tool for SWIDS framework.** For this contribution, we developed a proof of concept (PoC) for our framework using the Python-Scapy library and implemented it on a laptop running Kali Linux OS. The proposed framework is centralized and supports a plug-and-play implementation. This framework automatically identifies all clients connected based on a specified SSID and detects MC-MitM attacks within the targeted Wi-Fi network. Finally, we evaluated our SWIDS framework in a Wi-Fi based IoT environment under different traffic scenarios. This evaluation helped us identify potential frame loss that affects detection performance, especially with long-distance detectors. Based on our evaluation, we decided to extend the present framework to include a distributed intrusion detection system to enhance performance in a broad area.

This contribution addresses the objective **O3**. The results of the design and development of SWIDS are published as a research article entitled **"A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks"** in the **IEEE Access Journal**. This publication, which is an extension of the article presented in **Chapter 3**, forms Chapter 4 of this thesis.

- **C4. Designing and developing a Distributed and Cooperative Signature-Based Wireless Intrusion Detection System (DC-SWIDS).** The aim of this contribution is to enhance the performance of our SWIDS framework and expand its surveillance capabilities against MC-MitM attacks.

  - **C4.1 Designing of DC-SWIDS framework.** For this contribution, we enhanced our SWIDS framework by creating an Autonomous Detection System (ADS) that can be distributed in a Wi-Fi environment for a wider surveillance against MC-MitM attacks. Furthermore, distributed ADS nodes cooperate by exchanging status of attack data. This results in quicker detection and allows independent attack decisions in the places where ADS nodes are deployed. Message Queuing Telemetry Transport (MQTT) protocol is used for the communication among nodes.

  - **C4.2 Development of an open source tool for SWIDS framework.** Furthermore, we implemented the ADS nodes on single-board computers (Raspberry Pis) and evaluated them in real Wi-Fi-based IoT networks under different

testing scenarios. We also developed a graphical user interface (GUI) as a proof of concept for setting up an ADS node. Our evaluation demonstrated that the proposed distributed framework effectively overcomes potential frame losses and achieves a minimum average detection accuracy of 98% for MC-MitM attacks when deployed at various locations.

This contribution addresses the objective **O4** and the results of the design and development of DC-SWIDS have been submitted as a research article entitled **"A Distributed and Cooperative Signature-Based Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks"** to the **International Journal of Information Security, Springer.** This article forms **Chapter 5** of this thesis.

1.7 Overview of the PhD thesis

The reminder of this PhD thesis is organized as follows:

Chapter 2 presents the preliminary concepts and background information about MC-MitM attacks used in the rest of the thesis. It offers a detailed review of various MC-MitM attacks and provides a thorough analysis of the existing defense mechanisms against them. Additionally, it highlights various research challenges and problems associated with these attacks.

Chapter 3 presents how we theoretically and empirically designed and developed the attack signatures of MC-MitM attacks. It presents a classification of the different MC-MitM attack variants and proposes a detection system based on attack signatures.

Chapter 4 introduces the system architecture and functional units of the proposed signature-based wireless intrusion detection (SWIDS) framework for MC-MitM attacks. It illustrates the detection methodology and also provides the results of attack detection performance in a practical Wi-Fi based IoT environment.

Chapter 5 introduces the system architecture and functional units of the proposed distributed and cooperative signature-based wireless intrusion detection (DC-SWIDS) system for MC-MitM attacks, along with the results of attack detection performance in a practical Wi-Fi-based IoT environment.

Chapter 6 provides a discussion on thesis results, publications, and projects.

Finally, **Chapter 7** concludes the thesis and presents possible areas for future work.

2

Multi-Channel Man-in-the-Middle attacks against protected Wi-fi networks: A state of the art review

Expert Systems With Applications 210 (2022) 118401

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review

Manesh Thankappan [a,*,1], Helena Rifà-Pous [a,b,2], Carles Garrigues [a,b,3]

[a] Estudis d'Informàtica Multimèdia i Telecomunicació, Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Barcelona, Spain
[b] Center for Cybersecurity Research of Catalonia (CYBERCAT), Barcelona, Spain

ARTICLE INFO

Keywords:
Wi-Fi
WPA
Man-in-the-Middle (MitM)
Multi-Channel MitM (MC-MitM)
KRACK
Internet of Things (IoT)
Encryption
Security
FragAttacks

ABSTRACT

Multi-Channel Man-in-the-Middle (MitM) attacks are special MitM attacks capable of manipulating encrypted wireless frames between two legitimate endpoints. Since its inception in 2014, attackers have been targeting Wi-Fi networks to perform different attacks, such as cipher downgrades, denial of service, key reinstallation attacks (KRACK) in 2017, and recently FragAttacks in 2021, which widely impacted millions of Wi-Fi devices, especially IoT devices. To the best of our knowledge, there are no studies in the literature that holistically review the different types of Multi-Channel MitM enabled attacks and analyze their potential impact. To this end, we evaluate the capabilities of Multi-Channel MitM and review every reported attack in the state of the art. We examine practical issues that hamper the total adoption of protection mechanisms, i.e., security patches and Protected Management Frames (PMF), and review available defense mechanisms in confronting the Multi-Channel MitM enabled attacks in the IoT context. Finally, we highlight the potential research problems and identify future research approaches in this field.

1. Introduction

WLANs are broadly employable in several networking applications because of their flexibility, mobility, and availability. With the influx of the Internet of Things (IoT), Wi-Fi devices operating on the 802.11 standards are now gaining widespread deployment everywhere. Unfortunately, WLANs are susceptible to a broad array of wireless security attacks. Man-in-the-middle (MitM) attacks are a common form of security attack towards wireless networks that allow attackers to catch and manipulate communication between two end devices. One of the advanced MitM attacks is the Multi-Channel MitM (MC-MitM) attack that can manipulate the encrypted network traffic, as presented in (Vanhoef & Piessens, 2014). Since (Vanhoef & Piessens, 2014), MC-MitM attacks have been a trend in exploiting various Wi-Fi Protected Access (WPA) protocols in personal and enterprise networks. These kinds of attacks include denial of service (DoS), security downgrades, key reinstallations, and other vendor-specific exploits. The MC- MitM attack makes use of two different channels that facilitates the attacker to forward frames between both channels so that he can legitimately manipulate (e.g., block, delay, modify, inject, replay) encrypted frames between clients and the access point (AP) in a WLAN.

The Wi-Fi Alliance (WFA) and leading device manufacturers started noticing the MC-MitM attacks after the disclosure of a massive key reinstallation vulnerability (CVE-2017-13077) in the mid of 2017 (Vanhoef & Piessens, 2017). This was the first non-vendor specific vulnerability (as it is found in 802.11 standards) that could be exploited by MC-MitM enabled attack known as key reinstallation attack (KRACK), which abuses severe vulnerabilities, such as nonce and replay counter reuse during 4-way handshake mechanisms in the WPA and WPA2 certified devices. This vulnerability makes MC-MitM attackers more effective as they can trivially decrypt Wi-Fi frames, especially from Linux and Android devices. To resolve key reinstallation vulnerabilities, the Wi-Fi Alliance and some affected Wi-Fi chip manufacturers released patches. Available patches are only applicable to powerful Wi-Fi clients (e.g., laptops, smartphones, routers, etc.). However, many Wi-Fi devices cannot be patched because some companies do not provide them, especially IoT devices suffer from this issue. Some constraints like low computing capacities or specific network settings also impede the

* Corresponding author.
E-mail addresses: mthankappan@uoc.edu (M. Thankappan), hrifa@uoc.edu (H. Rifà-Pous), cgarrigueso@uoc.edu (C. Garrigues).
[1] ORCID: 0000-0001-8919-4857.
[2] ORCID: 0000-0003-0923-0235.
[3] ORCID: 0000-0002-7812-3401.

https://doi.org/10.1016/j.eswa.2022.118401
Received 7 June 2021; Received in revised form 28 May 2022; Accepted 3 August 2022
Available online 17 August 2022

adoption of patches on IoT devices. This situation pushes millions of WPA or WPA2 devices, especially IoT devices, to remain vulnerable to MC-MitM attackers. In 2019, a security research company tested several commercially available Wi-Fi devices and reported that 90% of them are vulnerable to key reinstallation attacks (Security Focus, 2019). Another recent exploratory study (Aug 2020) presented in (Freudenreich et al., 2020) critically indicates that overall, 65% of Wi-Fi and IoT devices tested are vulnerable to key reinstallation attacks. Regarding WPA3, although it provides improved security features in terms of encryption, it does not prevent KRACK on its own (Vanhoef, 2017b). This is because WPA3 executes the same 4-way handshake mechanism that is vulnerable in the same way as the one present in WPA and WPA2 protocols. The resilience of WPA3 devices towards KRACK also solely depends on the application of patches during the WPA3 certification process (Krischer, 2019).

In mid of May 2021, Vanhoef presented a set of new MC-MitM enabled attacks dubbed as FragAttacks (fragmentation and aggregation attacks) (Vanhoef, 2021a), which abuse serious security vulnerabilities (CVE-2020–24586,87,88) due to the lack of proper authentication in the aggregation and fragmentation features of 802.11 standards. This is another non-vendor specific vulnerability affecting every Wi-Fi device, including the new WPA3. FragAttacks enable attackers to inject packets into protected Wi-Fi networks and then capture clients sensitive data. WFA has released patches for these vulnerabilities, and other leading device vendors are currently releasing patches. The arrival of FragAttacks brings big concern in terms of securing IoT devices as such devices rarely receive patches and can experience the same difficulties as KRACK patching in upcoming years.

Generally, besides patches, another solution to counter various MitM or DoS attacks is the use of 802.11w standard or Protected Management Frames (PMF), which provides integrity protection for wireless frames (Philipp Ebbecke (Wi-Fi Alliance), 2020). However, many existing Wi-Fi clients in our home or office settings, especially IoT devices, may not always comply with PMF. A significant reason is that PMF was vendor-specific and was optional for currently available WPA or WAP2 devices. Only some Cisco devices provide client support for the PMF standard. A new survey on Wi-Fi security risks presented in (Reyes et al., 2020) critically points out that around 87% of analyzed routers do not comply with PMF standards.

The remarkable point is that MC-MitM attacks can easily circumvent PMF protection as attackers utilize certain pre-authenticated management frames which are not protected even when PMF is enabled. Once MC-MitM is acquired, attackers can plan for several attacks. For example, they can trigger FragAttacks or KRACK as the PMF standard itself is vulnerable to such attacks (CVE-2017–13081). Additionally, the MC-MitM attackers can exploit several inherent PMF vulnerabilities (e.g., channel switch attacks, jam genuine channel switch announcements, forge reassociation frames) more practically and eventually cause a potential deadlock or DoS on PMF-capable networks (Vanhoef et al., 2018). These attacks are hard to detect because the attacker requires merely a single forged frame for the impact.

Similarly, another pertinent issue is that, even though new WPA3 routers enter our domestic networks, they must be configured to operate in transition mode to accommodate many PMF incapable or legacy devices. In this case, MC-MitM attackers may target and hijack such devices connected to WPA3 routers and challenge their security. This situation may persist for several years because millions of WPA or WPA2 devices are currently deployed everywhere. However, it is not a good practice to close eyes from the risk of possible MC-MitM attacks.

Detecting MC-MitM attacks is challenging because the attacker acquires MitM position between an already connected client and AP in a WLAN without disconnecting clients from the legitimate network. Most importantly, the MC-MitM attacker uses a rogue AP that behaves as a normal AP in a WLAN. He neither floods the Wi-Fi medium with deauthentication frames nor performs any other dubious activities while acquiring the MitM position and tricks end devices to believe that they are communicating with each other directly. So to correctly differentiate between the normal and dubious activities, some prudent mechanisms are required. In mitigating MC-MitM attacks, some mechanisms have been proposed in the literature. Amongst such defense mechanisms, we perceive that operating channel validation (Vanhoef et al., 2018) and beacon protection (Vanhoef et al., 2020) mechanisms can considerably harden these attacks. However, these mechanisms still allow partial MitM attacks or block MC-MitM attacks if they originate from outsiders or unauthenticated users. The significant problem that persists is how to block potentially such malicious insider MC-MitM attacks, and this vulnerability remains open in all WPA standards, including WPA3.

Currently reported MC-MitM attacks so far impact WPA, WPA2, and WPA3 devices. FragAttacks are the most recent ones in the series of MC-MitM attacks. This shows that currently incorporated MC-MitM defense mechanisms in 802.11 standards are not yet really used in practice. Our analysis also revealed that most of the existing mechanisms are not flexible to implement in IoT environments because they mandate installing additional security modules, configuring their new solutions on home routers or every Wi-Fi client. We highlight the point that there are several IoT devices in a smart environment, and the defense mechanism cannot be based on the premise that all these devices will have to be modified, updated, or replaced by new ones. The technical overhead on ordinary people is also considerably high when deploying existing defense mechanisms due to complex configurations, setting up specific networks, firmware installation, etc. Traditional IDS like SNORT are also ineffective in confronting this kind of MitM attack. This is because SNORT works at the network layer and cannot detect MC-MitM attacks at the link layer.

The above issues shed light on the fact that preventing MC-MitM attacks can be difficult in practice, and especially if IoT devices have limited protections against them. Therefore, IoT environments need imperative developments against these attacks and are essential due to the increased influx of IoT devices to our smart environments.

Contributions of the Paper. The main contributions of the paper are:

- An in-depth evaluation of MC-MitM attacks capabilities in manipulating protected Wi-Fi communications, in particular, WPA, WPA2 and WPA3 networks, and examining whether attacks discovered for WPA2 are still possible in WPA3.
- A thorough review and a classification of MC-MitM enabled attacks.
- An analysis of possible security impacts of MC-MitM attacks.
- An examination of challenges in adopting general protection mechanisms such as security patches and PMF against MC-MitM attacks.
- A technical feasibility analysis of existing defense mechanisms for MC-MitM enabled attacks in IoT context.
- An analysis of potential research problems, challenges and future research approaches.

Organization. The paper's remainder is organized as follows. Section 2 briefly outlines protected Wi-Fi networks and fundamentals of MitM attacks. In Section 3, detailed technical setup and inner workings and classifications, specialities of MC-MitM attacks are presented. Section 4 reviews recent MC-MitM enabled attacks, examines significant difficulties in adopting security patches and PMF against MC-MitM attacks, and analyses how MC-MitM attacks impact new WPA3 networks. In Section 5, the existing detection mechanisms for combating MC-MitM attacks are reviewed followed by their technical feasibility analysis in the IoT context. Section 6 discusses identified research problems, challenges, and future research approaches in this field. Finally, Section 7 concludes our research analysis.

2. Protected Wi-Fi networks and MitM attacks

In this section, we explore various security protocols of 802.11 standards, including the PMF used for protecting Wi-Fi communication,

and highlight the related issues in terms of MitM attacks. We provide fundamentals of Wi-Fi based MitM attacks and evaluate how rogue AP MitM attackers manipulate protected Wi-Fi communication. In this paper, the term "manipulate" is used to represent the attacker's ability to reliably intercept and perform operations, such as exchanging, blocking, forging, modifying, replaying, injecting, or decrypting link-layer wireless traffic using the MitM position.

2.1. A security analysis of protected Wi-Fi networks

IEEE 802.11i standard defines protected Wi-Fi networks with more robust security solutions to the 802.11 standard. IEEE 802.11i is also known as a Robust Security Network (RSN) (Frankel et al., 2007). To provide link-layer protection for Wi-Fi communication under 802.11i, the Wi-Fi Alliance maintains three security certifications, namely WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access II), and WPA3 (Wi-Fi Protected Access III). As encryption or data confidentiality protocol, Temporal Key Integrity Protocol (TKIP) is used in WPA and is optional in WPA2, while WPA2 and WPA3 protocols mandate Advanced Encryption Standard (AES). As a data integrity protocol, WPA uses a Message Integrity Check (MIC) known as Michael algorithm (Beck & Tews, 2009), WPA2 and WPA3 mandate Counter Mode CBC-MAC Protocol (CCMP) for their personal networks, and the new Galois Counter Mode Protocol (GCMP) enhances WPA3 security for its enterprise networks (He & Mitchell, 2004; Vanhoef, 2017b). In this paper, instead of certifications, we may use terms such as devices, or networks interchangeably depending on context.

2.2. Connection establishment in WPA, WPA2 and WPA3 networks

According to 802.11i, when a client connects to a router or AP in a Basic Service Set (BSS) or WLAN, it passes through four phases: (i) network discovery, (ii) authentication, (iii) association, and (iv) 4-way handshake mechanism, as illustrated in Fig. 1. This connection establishment is also known as 802.11 State Machine (Frankel et al., 2007). Following, we briefly discuss the four phases.

2.2.1. Network discovery

In a WLAN, APs show their network presence by periodically broadcasting beacons. A beacon includes the SSID (Service Set Identifier) or network name, MAC address, channel, and other capabilities of the AP. Next, the client device scans and lists available networks so that the user can select the appropriate network and manually enter the Wi-Fi passphrase or pre-shared key (PSK) that was already configured in the AP. Important to note that this passphrase is stored or cached in the Wi-Fi chip of the client and is never transmitted or exchanged in any of the frames. With the selected SSID, the client sends a probe request frame to verify whether a specific network is available or not, and this activity begins with the state machine. In response to this, the AP sends a probe response frame by acknowledging the availability of SSID. This finishes the network discovery. The steps of this phase are common for WPA, WPA2, and WPA3.

2.2.2. Authentication

During the authentication, the AP verifies the client's identity (MAC address) and registers it in its cache. As shown in Fig. 1, the authentication phase has different steps according to the version of the security protocol. In WPA or WPA2, the client and AP exchange open authentication requests and response frames. Upon a successful authentication, a Pre-Master Key (PMK) is derived from the PSK on either side. On the other hand, the WPA3 protocol executes a new Dragonfly handshake (termed as Simultaneous Authentication of Equals, a.k.a SAE) by exchanging four authentication frames. Before this, both the client and AP generate a secret element known as Password Element (PWE) and two secret values. During the first two authentication frames (commit messages), the client and AP negotiate a PMK through Elliptic Curve

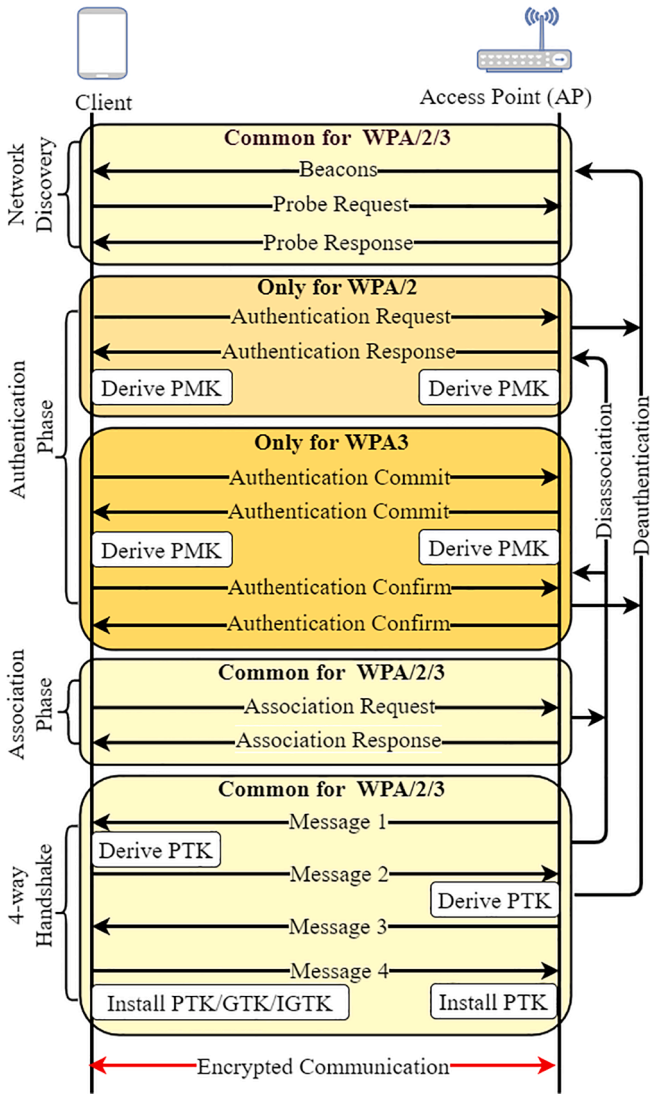


Fig. 1. Generalized connection establishment between the AP and client (Kohlios & Hayajneh, 2018; Vanhoef, 2017b).

Diffie–Hellman (ECDH) key exchange technique (Kohlios & Hayajneh, 2018; Vanhoef & Ronen, 2020). In the last two authentication messages, they confirm that both negotiated the same PMK. This way, the PMK is calculated using respective security protocol and cached on either device, maintaining the state machine. The generated PMK will be utilized in the 4-way handshake. After authentication, deauthentication frames from either client or AP will cause a disconnection from the network.

2.2.3. Association

As soon as the authentication ends, the client prepares to associates with the AP by forwarding an association request to negotiate required cipher suites such as TKIP/CCMP/GCMP. During the client's association, the AP keeps an association ID and sends an association response back. A client can be authenticated to many networks but can be associated with only one network at a time (Frankel et al., 2007). Note that with cached PMK, a client will be allowed to rejoin an already associated AP even after leaving the network, or a client can be quickly reconnected to the AP after an intermittent disconnection. Thus, the user or client does not need to enter a Wi-Fi passphrase again since the AP maintains its state machine or security association. This procedure is the same in WPA, WPA2, and WPA3. Like deauthentication, disassociation can occur at this stage, disconnecting the client. Finally, the 4-way handshake starts upon a successful association.

2.2.4. 4-Way handshake mechanism

The 4-way handshake mechanism is the same in WPA, WPA2, and WPA3 protocols, and involves exchanging 4 EAPOL (Extensible Authentication Protocol over LAN). During this handshake, the AP and client derive a Pairwise Transient Key (PTK), also known as a session key, which is then used for encrypting the actual communication between them. To derive PTK, the PMK is used with other parameters which are: AMAC represents AP's MAC address, CMAC represents client́s MAC address; AN represents AṔs random number, CN represents client́s random number; RC is the replay counter; PRF indicates Pseudo-Random Function. Finally, MIC (x, x, etc.) brings the Message Integrity Code created for the contents within the parentheses with derived PTK so that the AP or Wi-Fi client can verify whether this message is corrupted or not (He & Mitchell, 2004, Hiertz et al., 2010). Group-Transient Key (GTK) is independently derived at every AP and is the same for all the clients connected to it. Similarly, Integrity Group-Transient Key (IGTK) will be derived if PMF is enabled (see Section 2.3). Corresponding 4-way handshake message exchanges are summarized as follows.

- Message 1: AP → Client.
  The AP sends [AMAC address, AN, and RC] to the client. With these values, the client derives PTK, i.e., PTK ← PRF (PMK, AN, SN, AMAC, CMAC).
- Message 2: AP ← Client.
  Once PTK is derived, the client sends [CMAC, SN, RC, and MIC (CMAC, SN, RC)] to the AP.
- Message 3: AP → Client.
  Once message 2 is received, AP verifies MIC and derives PTK. The AP also derives GTK (Group Transient Key) and then the AP sends back [AMAC, AN, RC + 1, GTK and MIC (CMAC, SN, RC + 1, GTK)] to the client.
- Message 4: AP ← Client.
  Once message 3 is received, the client sends [CMAC, SN, RC + 1, and MIC (CMAC, SN, RC + 1)] to the AP to acknowledge reception of message 3 successfully. Consequently, both the AP and client will install PTK and GTK.

With the 4-way handshake, both the AP and client complete the state machine and stay connected. During this phase, deauthentication or disassociation can happen due to various reasons. Once end devices install security keys, the pairwise data communication between the AP and client will be encrypted (at the link layer) by the session key PTK using negotiated ciphers. The AP uses GTK to encrypt broadcast or multicast frames to communicate with every associated client.

As far as WPA and WPA2 are concerned, the foremost issue is that they are vulnerable to brute force or dictionary attacks, which aid attackers in retrieving security keys and potentially decrypt previously encrypted sessions. This happens because the generated PMK is the same for all clients. However, WPA3 solves this issue prominently by using a Dragonfly handshake that not only increases the entropy of the PMK but also ensures robust authentication/key exchange through Elliptic Curve Cryptography (ECC) and strong encryption through AES-GCMP. Therefore, offline dictionary attacks and the compromise of previous sessions (forward secrecy) are prevented since the derived PMK is independent of the PSK, and each client has a different PMK.

On the other hand, although data frames (actual communication between end devices) are protected using security protocols, all the management frames during the network discovery, authentication, and association phases are left unprotected as they are exchanged before negotiating security keys. Therefore, attackers can spoof such frames, impersonate the AP by setting up rogue devices and orchestrate several MitM attacks. For example, by spoofing the MAC address of the AP, the attacker can send deauthentication or disassociation frames to the client. Similarly, he can send a reassociation frame to the AP by spoofing the client. In either situation, the client gets disconnected from the legitimate network, resulting in DoS attacks. To counter these issues, the PMF standard was introduced.

2.3. Protected management frames (PMF)-IEEE 802.11w

The PMF or IEEE 802.11w standard was ratified in 2009 and became a part of 802.11i standard in 2014 (Wright, Charles V., Fabian Monrose, 2009). Although PMF has been around for a longer time, its market adoption was relatively low as it was an optional feature for existing WPA2 certifications. From 2018, WFA made PMF, a mandatory security requirement for new certifications of both WPA2 and WPA3 (Burke, 2018). When PMF is enabled, it protects some specific robust management frames, such as disassociation, deauthentication, and action frames (e.g., Spectrum Management). The two main amendments of PMF are:

1) A Message Integrity Code (MIC) is generated using the shared secret IGTK (Integrity Group Temporal Key) that encrypts broadcast or multicast robust management frames (e.g., deauthentication) for providing authentication and replay protection. MIC calculation is accomplished by Broadcast/Multicast Integrity Protocol (BIP).

2) Security Association (SA) Teardown Protection is added as an association spoofing protection mechanism to prevent spoofing attacks from tearing down an existing client association. This is accomplished with a SA Query procedure that provides protection against rogue APs or clients. It is a crypto protected probe message initiated by either party to verify the authenticity of (dis)association requests.

PMF would be effective only when both AP and client support it or every device in a WLAN supports it. However, unfortunately, most currently available WPA2 devices are not capable of this feature. Although some Cisco routers support PMF, it is rarely enabled in infrastructure networks due to enormous interoperability issues. It is also almost non-existent in IoT devices due to resource-intensive crypto operations. On the other hand, even though PMF ensures data origin's authenticity of specific robust management frames such as deauthentication or disassociation frames, it does not protect other pre-authenticated management frames, such as beacons, probe responses, authentication, or (re)association frames (Bertka, 2012). This fundamental conundrum still challenges the security of not only WPA2 but also WPA3 devices, and it allows attackers to introduce MitM attacks.

In the next section, we outline the procedures involved in performing MitM attacks and analyze MitM attacḱs capabilities in manipulating wireless traffic in a WLAN.

2.4. Fundamentals of MitM attacks in Wi-Fi networks

According to (Conti et al., 2016), a MitM attacker in Wi-Fi networks can eavesdrop on the wireless communication between two end devices and, in some cases, can even actively manipulate the data flow. To successfully implement MitM attacks in Wi-Fi networks, attackers follow general procedures, as shown in Fig. 2 (Kaplanis, 2015). During the first stage, information-gathering, the attacker may devise war driving tools (e.g., Kismet) to deduce useful identifiers (e.g., SSID, MAC address, and channel) about the AP and clients in a WLAN. Using the deduced information from this stage, the attacker sets up a rogue AP (also known as Evil-Twin) for masquerading as the real AP in the second stage, which is instrumental in achieving the MitM position.

In the third stage, the attacker tries to deceive the clients in a WLAN. To do this, firstly, the rogue AP transmits the strongest Wi-Fi signals to lure the clients and waits for any clients who accidentally connect to the rogue AP so that he can begin capturing their traffic. He also plans for a series of active attacks (e.g., deauthentication or disassociation attack) to disrupt communication to force clients (victims) to connect to the rogue network. Once victims get connected to the rogue AP, the attacker can actively intercept traffic in the final stage. In the next section, we analyze how rogue AP-based MitM attacks manipulate protected or encrypted link-layer traffic between a client and AP in a WLAN.

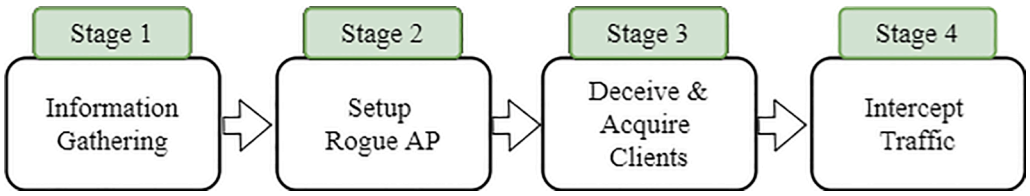


Fig. 2. General procedure for MitM attacks.

2.4.1. Rogue AP based MitM attack and protected Wi-Fi networks

Usually, rogue APs are devised to trick the client into connecting to separate networks other than real AP in a WLAN (Alotaibi & Elleithy, 2016). Here, we consider a rogue AP scenario (which we will refer to this as a traditional rogue AP MitM attack from now on) where the attacker acquires MitM position between the real AP and client, as depicted in Fig. 3. We also assume that the attacker knows the Wi-Fi passphrase as he is already connected to the real AP.

To acquire the MitM position, the attacker usually introduces his rogue device (e.g., laptop) between the client and real AP that generally operates with two Wi-Fi cards, a built-in card integrated into the device, and another one that can be a plug-and-play wireless card or a USB dongle. The plug-and-play card acts as the rogue AP by spoofing the real AP to the client, while the built-in card is usually associated with the real AP (Alotaibi & Elleithy, 2016; Roth et al., 2008).

Then the attacker creates a rogue protected network with the same SSID, MAC address, and known security key (Wi-Fi passphrase) used in the real network to trick the user into connecting to the rogue AP's network. Wireless packets are relayed between the plug-and-play card and built-in card using a bridged network connection or traffic forwarding for providing Internet connectivity to the victim. An example of a traditional rogue AP MitM attack can be found in (Yeahhub, 2018).

It is important to note that this traditional rogue AP MitM attack deletes the client's legitimate security association (original connection) with the real AP and forces it to perform a new authentication and association using a Wi-Fi passphrase with the attacker's rogue AP. This implies that a Wi-Fi passphrase must be known in order to perform such MitM attacks. Moreover, the attacker cannot manipulate any link-layer traffic between the client and the real AP as their connection is already broken. Therefore, once the MitM position is acquired, the attacker usually intercepts or manipulates the Internet traffic (between the client and web server) provided by the bridged connection or traffic forwarding between the plug-and-play card and built-in card. On the other hand, the bridged connection cannot be used to block or inject protected link-layer frames between the end devices. Most importantly, traditional rogue AP MitM attacks will not be successful if PMF is enabled. This is because spoofed deauthentication will be ignored while disconnecting the existing connection.

In contrast, MC-MitM attacks, our research focus, acquires the MitM position efficiently between an already connected client and the real AP without possessing a legitimate Wi-Fi passphrase and deleting the original security association between them. Moreover, the use of different channels enables such attackers to cleverly spoof end devices and actively manipulate the encrypted link-layer traffic of a single connection between the client and the real AP. MC-MitM attacks can also acquire MitM positions in PMF environments.

3. Technical setup and inner workings of Multi-Channel MitM attacks

In this section, we elicit the technical setup and inner-workings towards acquiring the MC-MitM position between Wi-Fi devices. Our main aim is to evaluate the capabilities of MC-MitM attacks in manipulating protected Wi-Fi networks. We compare the characteristics of MC-MitM with traditional rogue AP-based MitM attacks in Wi-Fi networks. Finally, we analyze how MC-MitM attacks become possible in WPA3 networks and related issues.

3.1. Overview of MC-MitM attacks

Vanhoef et al. introduced the MC-MitM attacks against protected Wi-Fi networks in 2014 (Vanhoef & Piessens, 2014). In this kind of attacks, the main goal of the attacker is to obtain a MitM position between two already connected wireless devices without breaking their original security association and then to forward or exchange encrypted frames between them reliably. Once the attacker acquires this MitM position, he can effectively manipulate wireless frames in a way that is entirely legitimate to the victims. There are two prominent advantages in using a MC-MitM position: (1) victims remain unaware of the attack since their original connection or current security association is not disturbed; (2) attackers can bypass new authentication and association with the real AP (Chi et al., 2020). The latter one is more significant as the attacker does not hold a pre-shared Wi-Fi passphrase, which is the main parameter for deriving the session key during a 4-way handshake. To enter the network using the MitM position, the attacker uses two different channels (therefore, named as Multi-Channel-MitM) to

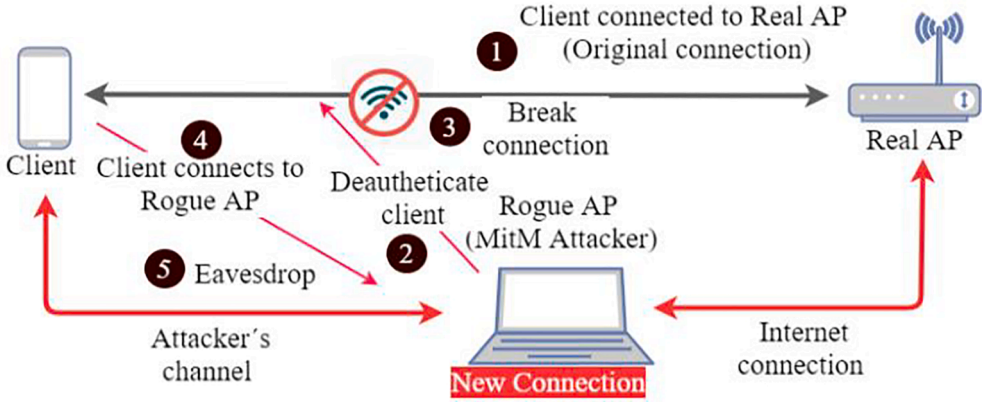


Fig. 3. Traditional rogue AP based MitM attack.

simultaneously communicate with both the client (victim) and real AP, as shown in Fig. 4.

As shown above, in the MC-MitM setup, the attacker cleverly spoofs communicating end devices (client and real AP) respectively on an on-side channel, which eventually drives the end devices to negotiate the same session key during a 4-way handshake mechanism. Besides, the attacker ensures that the client and real AP will never communicate directly through their original connection as he exchanges the specific communication between end devices with the help of a fake connection formed using two different channels. However, acquiring the MC-MitM position is a complicated procedure in protected wireless networks due to the 4-way handshake mechanism. The reason is that the attacker has to manage negotiated session keys derived from parameters, including the MAC address of the AP and client while maintaining the current or original security association between them. To carry through these conditions, a MC-MitM attacker performs the following two intriguing procedures: 1) Setup rogue interfaces for spoofing the victims; 2) Force the victims to switch to rogue channels. We demonstrate the inner workings of these two procedures, respectively, in Sections 3.2 and 3.3.

3.2. Rogue interface setup for spoofing the victims

This section demonstrates how the MC-MitM attacker sets up rogue interfaces for obtaining a MitM position between a legitimate connection, as shown in Fig. 5. Then Fig. 6 depicts how this legitimate connection is tweaked into the MC-MitM attack setup using spoofed interfaces. At first, the attacker inserts a laptop with a dual interface setup that simultaneously clones the targets, i.e., a real AP and a client (e.g., mobile devices, laptops, tablets) on different channels.

On the one hand, the first interface clones ESSID (Wi-Fi network name), MAC address, and other necessary parameters and spoofs the real AP for the client. On the other hand, the second interface spoofs the client by cloning the client's MAC address for the real AP. These two interfaces (with Wi-Fi antennas) must be in a physically reachable range (preferably 1–2 m) to effectively relay frames between different channels. The real AP is now cloned on a channel (channel B) other than the real channel (channel A) to connect with the client. This is an essential requirement because using the same MAC address as the real AP on the same channel (channel A) is impossible since the targeted client and real AP are already communicating with each other. Moreover, the rogue client (interface 2) needs to work on the same channel (channel A) of the real AP to show its presence on the real channel itself. Finally, to manage acknowledgment frames (ACK), the attacker modifies the firmware of interface 2 such that the rogue client will send ACKs when it receives unicast frames from the real AP. Once masquerading is complete, the rogue client (interface 2) can listen on channel A for the real AP, while the rogue AP (interface 1) listens on channel B for the client. Cloning two different interfaces in this way allows the interfaces to copy and exchange all frames from one channel to another, which drives both the client and real AP to negotiate the same session key during a 4-way handshake process. In the next section, we explain how end devices negotiate the same session key.

3.2.1. Steps to negotiate the same session key

As mentioned previously, since the MC-MitM attacker does not delete the original security association between the client and real AP or does not create a new connection using a Wi-Fi passphrase, the client and real AP continue to maintain their security association (current state machine) and retain details about PMK (a hash value derived from Wi-Fi passphrase and SSID) and association identifiers (association ID) in the state tables stored in the cache of their Wi-Fi chips (Frankel et al., 2007). To acquire the MitM position, the attacker first forces the client to connect to it. While forcing the client, the attacker transmits already collected beacons of real AP. When the client sees such beacons on channel B, it recognizes that the network is already authenticated or connected (as per the preferred network list) and sends a probe request with a selected SSID. Consequently, the attacker's rogue AP sends a custom probe response to the client on channel B, making the client to send an authentication request frame to it. At this moment, the rogue AP collects that authentication request frame and retransmit it on channel A using the rogue client. The real AP accepts it, and in response, it sends an authentication response frame on channel A, which the rogue client collects and retransmits on channel B. In the same way, association frames are exchanged.

Following a successful association, the real AP initiates the 4-way handshake. At this moment, as explained above, the rogue client and rogue AP setup collects each handshake message from its originating channel and retransmit it on another channel. Even though handshake messages are exchanged between two different channels, they will have a valid MIC (from message 2) when processed by the real AP. As a result, the client and real AP derive a new and same PTK (session key) on respective sides. Moreover, the real AP honors all these exchanged frames. This is because 1) real AP remembers the client's original security association; 2) frames are transmitted on the same operating channel (channel A) of the real AP. Once the session keys are negotiated, the attacker manages all the communication (data frames) between end devices through his MC-MitM setup so that he can reliably block, delay, buffer, modify, inject, or replay encrypted wireless frames. In this way, the attacker bypasses the need for new authentication and association using the Wi-Fi passphrase and achieves the MC-MitM position.

Although the MC-MitM position forces end devices to negotiate the same session keys, the attacker cannot acquire those keys as he is merely exchanging encrypted frames between two channels. Therefore, a MC-MitM position cannot decrypt any traffic passing through it on its own. Instead, the attacker employs the MitM position to exploit specific known vulnerabilities in WPA or WPA2 to potentially decrypt wireless traffic, as concisely discussed in Section 3.4.

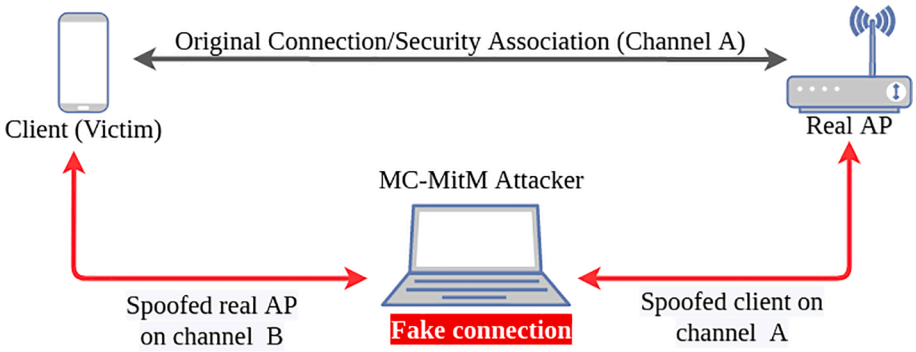


Fig. 4. MC- MitM attack.

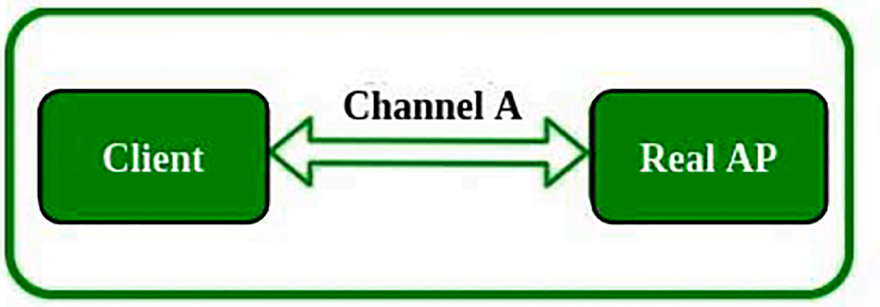


Fig. 5. Legitimate connection.

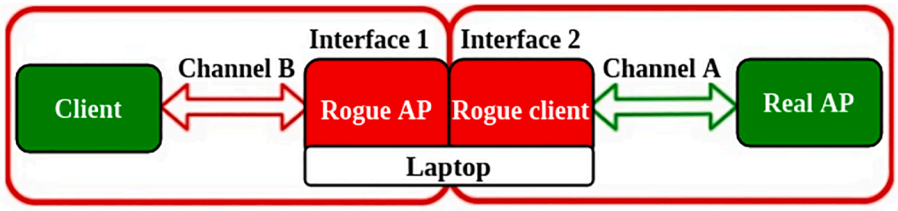


Fig. 6. MC- MitM attack setup.

3.3. Forcing the victims to switch to rogue channels of interfaces

As far as the real AP is concerned, it always transmits and receives frames on its operating channel (channel A). In the previous section, we explained how the MC-MitM attack setup uses interface 2 (rogue client) to communicate with the real AP and retransmit its frames on another channel (channel B) using interface 1. In this section, we demonstrate how the attacker uses rogue AP (interface 1) to force the client to connect to the rogue AP on its channel without deleting its current security association with the real AP. In terms of forcing clients to connect to the attacker's channel, we divide MC-MitM attacks into two variants: (1) base variant and (2) improved variant. We use these types later to classify existing multi-channel attacks in Section 4.

3.3.1. Base variant

This is the first MC-MitM attack variant presented by (Vanhoef & Piessens, 2014). In this variant, the attacker first constantly jams the original channel (channel A) of the real AP until the targeted client connects to his rogue channel (see Fig. 7). This is accomplished with commodity hardware capable of jamming Wi-Fi frames on a specific channel. Due to jamming, the client loses connection from real AP that is on the real channel (channel A). Meanwhile, the attacker with the rogue AP advertises beacons on rogue channel (channel B) to trick the victims into connecting to it. More specifically, the MitM attacker copies beacons of real AP from the real channel and retransmits them on the rogue channel.

Note that the jamming does not break the original security association. Instead, it just makes target networks unavailable for some time. As per the 802.11 standards, a client will always choose an available network or a network with the strongest signal. Therefore, victim switches to the rogue AP's channel and starts transmitting data on it. Additionally, the attacker observes specific probe requests from the client and instantly replies with custom probe responses to force it to switch to his channel. As soon as the client switches to the rogue channel, the attacker stops jamming.

As of now, the attacker acquires the MitM position, and he starts exchanging frames between the client and the real AP. This base variant can also attack PMF capable devices because management frames such as beacons or probe responses are not protected even if PMF is enabled (recall Section 2.3). We implemented and tested the base variant by using the Modwifii tool (Vanhoef, 2015).

3.3.2. Improved variant

This variant appeared with several improvements over the base variant and was also proposed by (Vanhoef & Piessens, 2018). With this improved variant, the MC-MitM attacker uses channel switch

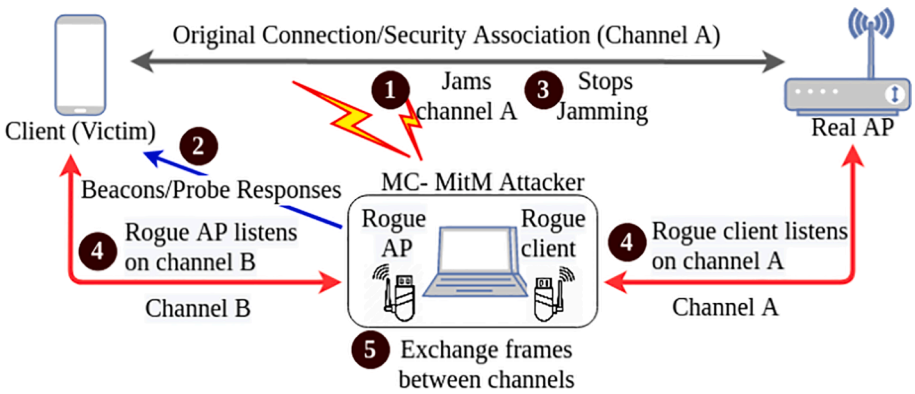


Fig. 7. Multi-Channel MitM Attack- Base variant.

announcements (CSA) to trick the client into connecting to his rogue channel. CSAs can be transmitted by inserting a CSA information element inside beacon frames, probe response frames, and action frames. Like the base variant, the improved variant also sends beacons or probe responses with spoofed CSA to trick both regular and PMF clients, whereas action frames are protected when PMF is enabled. Once the client receives CSAs, it will instantly switch to the rogue channel so that the attacker starts exchanging frames between the client and the real AP. Fig. 8 demonstrates the working of MC-MitM improved variant attacks.

Utilizing CSAs is reliable and does not disturb the current security association. It is a normal activity of APs in certain conditions (e.g., noise or congestion) that the clients cannot decline. Moreover, only a few CSAs (max 4 or 5) are enough to force the victims for the desired channel change. Fig. 9 depicts the structure of the CSA information element. The channel switch mode field regulates whether a wireless client can continue (when the mode is 1) or stop (when the mode is 0) sending information on a particular channel. The new channel number field indicates the expected channel to which the clients must go. The channel switch count field represents the remaining number of beacon interval to wait (a zero value indicates that channel switch is imminent) for a client before a channel switch.

Since CSAs can instantly switch channels of clients, channel jamming is not required in this variant, which considerably decreases attacker's efforts. Additionally, the attacker can spoof CSAs to the client to switch back to the real channel after abusing it. In any case, the client (victim) remains unaware of the attack. All combined, the MC-MitM improved variant increases impacts of attacks. We implemented and tested the MC-MitM improved variant attack by using the MitM channel package (Lucas Woody, 2018). In Table 1, we summarize the features of MC-MitM attack variants.

3.4. *Decrypting Wi-Fi frames using the MC-MitM position*

According to the IEEE 802.11 standard (Hiertz et al., 2010), performing decryption and encryption of Wi-Fi frames requires generating the session key (PTK) during a 4-way handshake mechanism. In section 3.2, we have seen how MC-MitM attackers manage to force end devices to negotiate the same session key without possessing a pre-shared Wi-Fi passphrase. Furthermore, we indicated that a multi-channel attacker has no access to those negotiated keys. This is a significant challenge because decrypting frames requires the knowledge of a particular session key. Even so, the MC-MitM attacker can achieve the above challenge in many ways. In previous MC-MitM attacks on WPA, the attacker abused specific weaknesses in encryption algorithms (e.g., MIC key derivation vulnerability in TKIP) so that he would be able to decrypt wireless frames (Vanhoef & Piessens, 2014). However, such decryption technique was a hard-to-win race condition since the attacker had to predict several parameters; moreover, he could decrypt only some arbitrary frames. On the other hand, with the disclosure of key reinstallation vulnerabilities in WPA2 standards, MC-MitM attackers could decrypt comparatively large numbers of packets in a short period irrespective of data confidentiality protocols used in Wi-Fi networks. Therefore, we show how key reinstallation vulnerabilities presented in (Vanhoef, 2017b) allow attackers to decrypt Wi-Fi frames of a particular communication session between end devices.

Regarding the key reinstallation vulnerability, the major flaw is in the WPA2 standard that makes every Wi-Fi capable device reset nonce and packet counters of data confidentiality protocol. This happens automatically whenever a session key (re)installed on the client-side during a 4-way handshake. This means that clients are already reusing nonce values even without an attacker being present. Fig. 10 depicts how encryption works generally in a Wi-Fi network.

As per Fig. 10, once the session key is negotiated, it will be combined with the transmitter's MAC address and the nonce value (packet number), which is incremented by one for every transmitted frame, and eventually a unique per packet key is derived (Vanhoef, 2018). This per packet key is fed into a stream or block cipher (encryption algorithm) to generate the corresponding keystreams and is then XORed with the plaintext packet payload to create the ciphertext or encrypted data corresponding to a particular frame. Finally, the nonce value is also appended to the header of the frames so that the receiver will be able to decrypt the frames. In this way, a nonce value is used to form a unique per packet key. An essential requirement here is that under a particular session key, the nonce value should only be used once. If the encryption algorithm ever reuses a nonce value, it will generate the same per packet key and yield the same keystreams. This is the major vulnerability that is wisely exploited by MC-MitM attackers to decrypt the Wi-Fi frames effortlessly.

Fig. 11 shows the technical representation of how a MC-MitM attacker can decrypt Wi-Fi frames. During stage 1, the MitM attacker exchanges the first three handshake messages between channels without any modifications. Actual MitM attack will start from stage 2, where the MitM attacker blocks the message 4 from the client and does not forward it to the AP. From the client's perspective, the handshake is completed, and so it installs the session keys (PTK and GTK) and initializes its nonce and replay counter values to zero as per Wi-Fi standard. Since the AP has not received message 4, it retransmits message 3 to the client in order to continue the handshake progress, which will be then forwarded by the MitM attacker to the client. Note that, as per 802.11 standards, if the AP does not receive message 4 because of reasons like noise or congestion in the network, it will always retransmit message 3. Consequently, the client sends message 4 (with a nonce value one as incremented due to the new frame) and is in encrypted form since the client has already installed the session key. Following the sending of message 4, the client again installs (reinstalls) session keys.

When a key is reinstalled, the nonce (packet number) and replay counter values are reset to zero. This means that if the client sends another data frame, it will again use the old nonce value one and thus

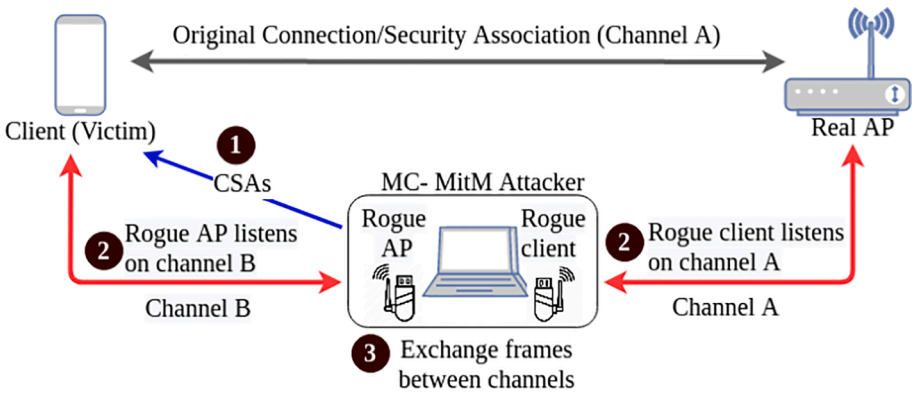


Fig. 8. Multi-Channel MitM Attack- Improved variant.

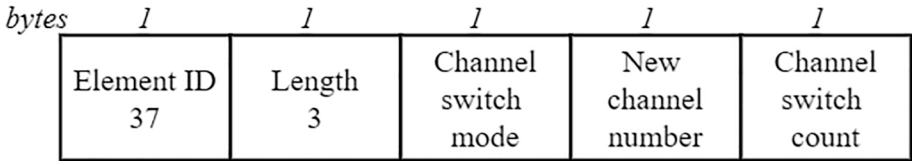


Fig. 9. Structure of a CSA element (IEEE 802.11 Standard, 2012).

Table 1
Comparison of MC-MitM attack variants.

Characteristics	Base variant	Improved variant
Employ beacons	Yes	Yes
Employ probe responses	Yes	Yes
Employ action frames	No	Yes
Needs jamming to launch attack	Yes	No
Ability to attack PMF clients	Yes	Yes
Cost effective method	No	Yes
More reliable method	No	Yes
More impactful method	No	Yes

uses an already-in-use session key (per packet key) for encrypting the data frames. Reusing the nonce in messages (as shown using green arrows in stage 2) causes the same keystreams to be reused.

At this stage, the multi-channel attacker starts abusing the nonce reuse scenario to recover the keystreams corresponding to the nonce value one. To do so, he performs the following: first, the attacker copies message 4 (M1) and encrypted message 4 (E1) to X-OR them to learn the keystream (KS1) belongs to the nonce value one. The reason for this is, the X-OR operation between plaintext and its encrypted message gives the keystream for that encryption. Second, the attacker copies encrypted data frame (E2) in stage 2, which also uses nonce value one due to key reinstallation, meaning that it might have used precisely the same keystream (KS1). Finally, the attacker again performs an X-OR operation

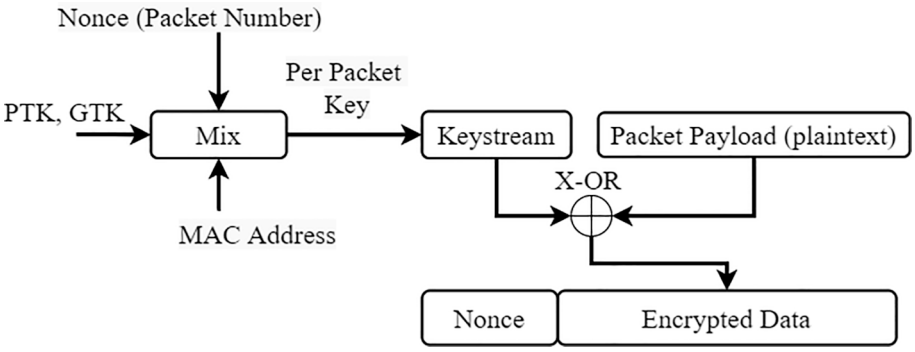


Fig. 10. Generalized encryption procedure in Wi-Fi.

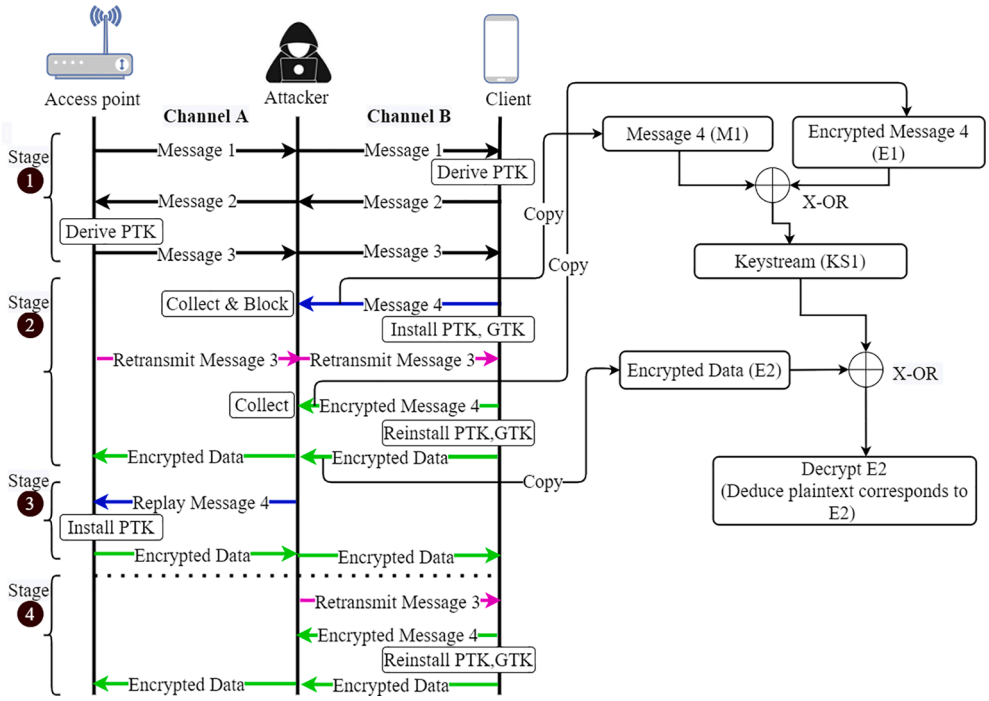


Fig. 11. Key reinstallation attack using the MC-MitM position.

between KS1 and E2 to get the plaintext corresponding to the encrypted data (E2).

In stage 3, the MitM attacker replays the already collected message 4 (blue arrows) towards the AP. The AP then accepts this replayed message 4 since the replay counter was reset during the last key reinstallation and begins sending encrypted data using an already-in-use session key, which can also be decrypted easily by the MitM attacker. Similarly, in stage 4, the attacker can force key reinstallations by replaying message 3 (pink arrows) retransmitted during stage 2. We remark that a key reinstallation attack enables decryption of just an encrypted message with a nonce value one. To decrypt the client's subsequent messages, the attacker must replay message 3 to induce nonce and replay counter reset during the key reinstallation attacks. By forcing the key reinstallations continuously in this manner, the attacker can decrypt a greater number of Wi-Fi frames. These frames can be a part of some TCP connections when user crawls websites or exchanges personal data.

Interestingly, (Chi et al., 2020) showed how MC-MitM attackers could capture Wi-Fi frames between two legitimate devices and then directly decrypt Wi-Fi frames on-the-fly using an open-source library, such as pyDot11. In this case, the attacker holds the pre-shared Wi-Fi passphrase, meaning that he is an insider and tries to decrypt a particular communication session between clients and the AP in the same WLAN.

3.5. Obtaining Wi-Fi data using the MC-MitM position

With the advent of recent aggregation and fragmentation security vulnerabilities found in the 802.11 standards (Vanhoef, 2021a), MC-MitM attacks become more widespread and practical to trigger FragAttacks towards WPA, WPA2, and the new WPA3 networks. FragAttacks enable the attackers to legitimately inject specific Wi-Fi frames and then obtain user's sensitive data. In this subsection, we show how FragAttacks leverage the MC-MitM position to intercept and obtain useŕs sensitive data.

In Wi-Fi, sending small Wi-Fi packets is inefficient because every frame must have a header and separately acknowledged, which may often induce high overhead on Wi-Fi chips. Therefore, small packets are aggregated into a larger frame containing multiple packets with the frame aggregation feature. Every Wi-Fi frame header contains an aggregation flag that indicates whether the frame payload contains a single (normal) packet or multiple aggregated network packets. Nevertheless, the major flaw is that the frame aggregation flag in the Wi-Fi header is not authenticated. This allows the attacker to flip the respective flag and trick the victim into processing encrypted frames by injecting frames towards him. Fig. 12 illustrates the aggregation attack in Wi-Fi.

During stage 1, the attacker acquires the MC-MitM position between the client (victim) and AP. He also sets up a fake DNS and web server for impersonating websites and Internet access for the client. In stage 2, the attacker tricks the client into connecting to his web server. This is accomplished by sending an email to the client, and when clicked, it causes downloading an image from the attacker's web server, establishing a TCP connection with the web server. The attacker manages this TCP connection to send a malicious TCP packet (IPv4 packet) to the client (stage 3). In stage 4, the AP encrypts the injected IPv4 packet as a normal frame and forwards it to the client. Afterward, the MC-MitM attacker subsequently identifies this frame and flips the aggregated flag before forwarding it to the client (stage 5).

On the other hand, the client will not detect this aggregated flag due to the design flaw. Therefore, the frame becomes an A-MSDU (Aggregate MAC Service Data Unit) frame so that the attacker can inject IP packets as subframes. When the client processes such aggregated frames, it will be tricked into connecting to the fake DNS server. The injected IP packets can be ICMP router advertisements or DHCP packets. Once the client is connected to the attacker's DNS server (stage 6), he can intercept all the client's IP traffic and obtain sensitive data (e.g., log-in details), especially while using insecure websites.

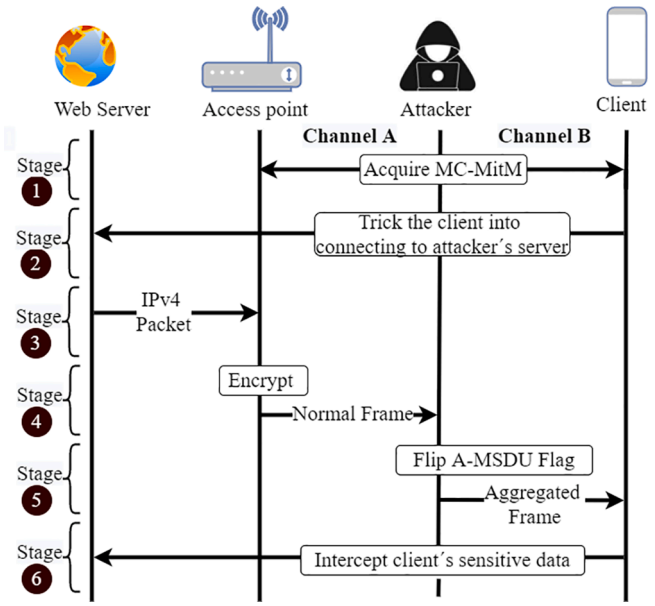


Fig. 12. Aggregation attack using the MC-MitM position (Vanhoef, 2021b).

Regarding Wi-Fi fragmentation, it is the process by which large frames are split into smaller frames in order to avoid the chances of frames being corrupted. This process also facilitates the retransmission of specific lost frames whenever required. There are two significant flaws discovered concerning the fragmentation allowing the revelation of victim data.

1. Even though the fragments of a frame are encrypted using the same key, there is no verification procedure (ensuring whether the same key encrypts the received frames) at the receiver. The sequence number field in a fragment is also not authenticated. As a result, attackers can abuse the lack of verification to inject and mix frames with different keys (with previous sequence numbers), which will be reassembled by the receiver (see Fig. 13).
2. The fragment cache is not cleared when clients (re)connect to particular Wi-Fi network. Therefore, this flaw allows the attacker to inject frames into the fragment cache, which will be reassembled with the clienťs fragments (see Fig. 14).

As shown in Fig. 13, the attack starts with acquiring the MC-MitM position during stage 1. In this stage, the client is first tricked into visiting an attacker-controlled website. For example, the attacker may send phishing emails, show third-party advertisements, or posts on blogs the client may visit, by social engineering the user activities, and load the corresponding Internet resource (web pages) on the attackeŕs web server. The main goal of this step is to create an attacker-destined packet (i.e., a packet with the destination IP address, which in this example is 3.5.1.1). When the client visits such long web pages or URL, the resulting packets will be split into two fragments (Frag 0 and Frag 1) as highlighted using green arrows. Note that fragments of the same frame will have the same sequence number s and incremental packet number n, and the session key k encrypts the fragments. The sample contents of these fragments are shown using dotted red arrows. The MC-MitM attacker detects and collects these fragments according to their unique length and only forwards the first fragment (Frag 0) to the AP. Upon receiving this fragment, the AP decrypts this fragment and stores it in its cache or memory.

During stage 2, the attacker forwards all other normal traffic without the packet number to ensure that the first fragment is never removed from the AṔs cache. He also waits for session key renewal after a 4-way handshake. The attacker can predict the rekey as it occurs in regular

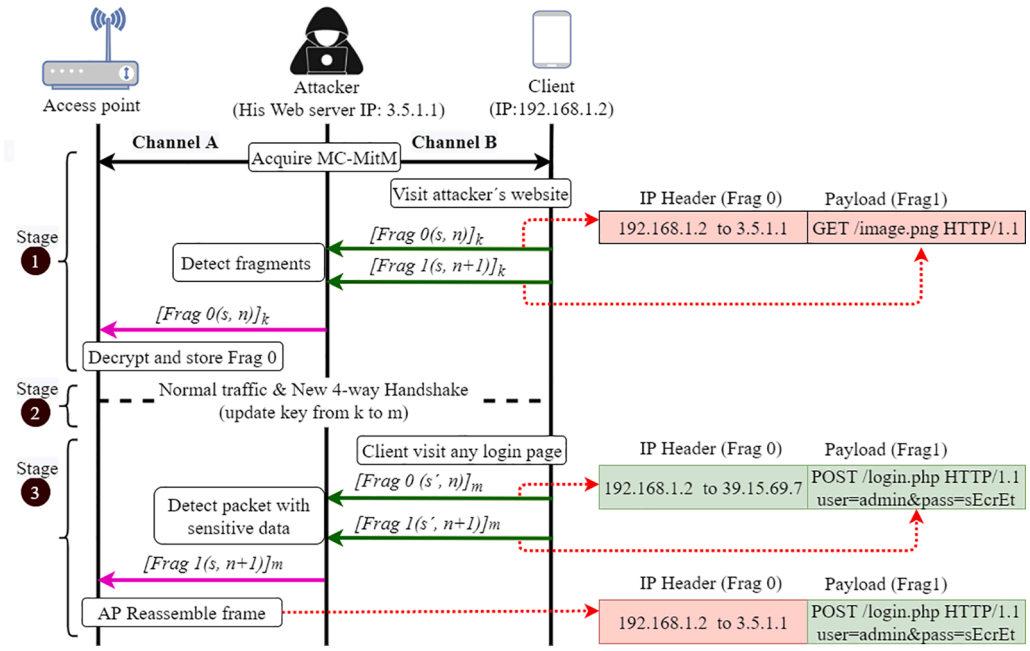


Fig. 13. Fragmentation mixed key attack using the MC-MitM position (Vanhoef, 2021a).

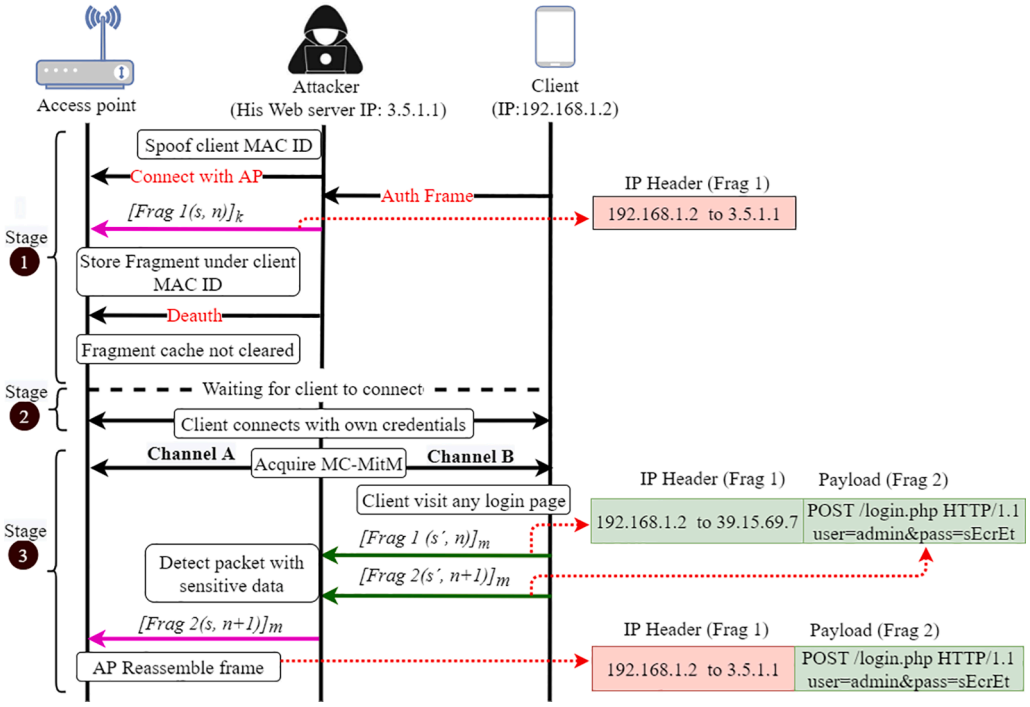


Fig. 14. Fragmentation cache attack using the MC-MitM position (Vanhoef, 2021a, 2021c).

intervals. By rekeying, packet numbers of the encryption protocol will be reset to zero. With these assumptions, stage 3 begins. Here, when the client visits any web page (having IP address, which in this example is 39.15.69.7) and provide log-in details through that particular web page, the corresponding IP packet (i.e., HTTP POST request) is split into two fragments and encrypted using the new session key *m*. At this moment, the MC-MitM attacker identifies those fragments with sensitive data and only forwards the second fragment (Frag 1) by tweaking its sequence number to *s* as the one used with the first fragment sent during stage 1. However, the AP combines both fragments (highlighted using pink arrows) into a new reassembled frame due to the design flaw. Since the attacker-destined packet is now combined with the useŕs sensitive data, it will be sent to the attackeŕs web server.

In the fragmentation cache attack, as illustrated in Fig. 14, the attacker basically targets enterprise networks such as eduroam, where each user has a unique username and password. In the first stage of the attack, the attacker accesses the network with his credentials. He also waits for an authentication request from the client (victim) and immediately injects an IP packet (Frag 1) to the AP by spoofing the client's MAC address. The goal of this packet injection is to create an attacker-destined packet with a destination IP as 3.5.1.1. Consequently, the AP decrypts this attacker-destined packet and keeps it in its memory or

cache with the client's MAC address. Then the attacker leaves from the AP with a deauth frame. Due to the design flaw, the attacker-destined packet remains in AP's cache even though the attacker disconnects from the network.

In stage 2, the attacker oversees that he never sends any frame to AP with sequence numbers to ensure that the injected frame is not cleared from its cache. He also waits for the client to normally connect to the AP by using valid credentials. In stage 3, soon after the client connects to the AP, the attacker establishes the MC-MitM position between them. The attacker now waits for the client to visit any web page and formation of two fragments (as illustrated in stage 3 of Fig. 13). Ultimate goal of the MC-MitM attacker here is to identify fragments (Frag 1 and Frag 2) and only forwards the second fragment to the AP. Afterward, the AP wrongly reassembles the previously injected attacker-destined packet with number n during the stage 1, with the newly forwarded packet with number $n + 1$ (both highlighted as pink arrows) into a single frame. This happens because the identities like MAC address and sequence number of fragments are the same. Therefore, the design flaw exploited here is that the AP does not maintain identities of fragments in enterprise networks when users (re)connect to a particular network. Eventually, the reassembled frame is sent to the attacker's server, revealing the user-sensitive data. The fragmentation cache attack is also possible against clients. In such cases, the attacker injects malicious IP packets towards clients to trick them into connecting to a fake DNS server even if clients are associated with trusted personal networks, such as home networks, coffee shops, where the Wi-Fi passphrase is publicly known to every-one.

We emphasize that the revelation of data is possible with FragAttacks as long as the client uses insecure websites that follow plaintext HTTP. Even if HTTPS is used, MitM attackers may use tools like sslstrip to bypass this upper-layer security. Therefore, nowadays, it is necessary to ensure that the website is HSTS (HTTP Strict Transport Security) compliant. Unfortunately, only very few websites dictate the use of HSTS for web communications as per the latest statistics (W3Techs, 2021). However, the aggregation and fragmentation vulnerabilities enable the attacker to inject any packets (unencrypted packets) based on his choice into a protected Wi-Fi network and pollute communication. On the other hand, such attacks are not possible with any other tools under normal conditions.

3.6. Other special features of MC-MitM attacks

In this subsection, we present certain special features of MC-MitM attacks in manipulating protected Wi-Fi networks.

3.6.1. Virtual interface support

Using a virtual interface support (a hardware technology), the rogue AP or interface 1 (see Fig. 6) employed in MC-MitM attacks can listen to multiple MAC addresses or clients simultaneously. Therefore, MC-MitM attackers can target or abuse more than one client at a time and can engender more security impact in practice (Vanhoef & Piessens, 2014).

3.6.2. Detect/exploit logical vulnerabilities

The MC-MitM position can be used to detect or test any logical vulnerabilities or cryptographic implementation bugs (e.g., reusing nonces, skipping handshake messages) present in Wi-Fi handshake mechanisms (Vanhoef et al., 2017). The attackers can then exploit such vulnerabilities to perform attacks like authentication bypass, DoS, chop-chop attacks, or downgrade attacks. Key reinstallation attacks and FragAttacks are well-known attacks that exploit cryptographic vulnerabilities in various handshake mechanisms or Wi-Fi aggregation and fragmentation capabilities. On the other hand, the MC-MitM position can be used to perform traffic analysis in protected Wi-Fi networks as part of defensive security analysis.

3.6.3. Jam Wi-Fi using USB dongle

The attacker uses a portable and cheap USB jammer to selectively (target specific frames) jam MAC-layer traffic on specific channels (Vanhoef & Piessens, 2014), which is comparatively difficult to be identified by using IDS systems (Gong et al., 2020). This jammer can be implemented even on a smartphone. The MC-MitM attackers appropriately use reactive or constant jamming to block or delay wireless traffic reliably.

3.6.4. Legitimate behavior of the MC-MitM attacker

In both MC-MitM variants, the attacker acquires MitM position without deauthenticating the victim from the real AP. According to our analysis, the attacker does not conduct any forms of flooding attacks using spoofed beacons or any other frames while acquiring the MitM, instead, it collects the beacons of real AP and retransmits them on rogue AP's channel. After acquiring MitM position, the attacker exchanges encrypted or manipulated frames, facilitating end devices to communicate through the attacker's MC-MitM setup as if they are communicating with each other directly. Finally, the victim can even rejoin the real AP after withdrawing the MC-MitM position since the attacker did not force the end devices to destroy their security association.

3.6.5. Trigger attacks from farther

To trigger MC-MitM attacks, the attacker need not be always close to the victim. He can use special directional antennas from farther (1 or 2 miles) and act as a repeater to obtain the MitM position and then relay the wireless frames from the AP to the victim (Vanhoef, 2018; Vanhoef et al., 2018). The attacker can also trigger attacks by cloning a far-away network and forward frames over the Internet by using specific TCP connections (Vanhoef & Piessens, 2014). However, these attacks are possible only if the attacker has prior knowledge about the network that the victim is supposed to connect. Recently, (Louca et al., 2021) demonstrate the feasibility of using channel switch announcements to acquire MitM from relatively longer distances even with the low signal strength.

In Table 2, we compare the essential characteristics of MC-MitM attacks with that of traditional rogue AP MitM attacks.

3.7. Analysis of MC-MitM attacks in WPA3

As we highlighted in Section 3.3, since MC-MitM attack variants can circumvent PMF protection and manipulate the protected communication on WPA2 devices, MC-MitM attacks can also affect WPA3 devices. This is possible because the connection establishment process is the

Table 2
Comparison of MC-MitM attacks with traditional rogue AP MitM attacks.

Characteristics	MC-MitM	Traditional rogue AP MitM
Main Objective	Acquire MitM position between an already client and the AP.	Disconnect the client from the AP and create a new rogue network having the same Wi-Fi password as a real AP.
Num. of Interfaces	Two: for spoofing AP and the client.	Two: Spoofing as AP and connecting Internet.
Ability to relay	Yes	Yes
Ability to manipulate link-layer encrypted traffic between the client and real AP	Yes	No
Ability to attack PMF clients	Yes	No
Ability to attack multiple clients	Yes	No
Ability to trace logical vulnerabilities	Yes	No
Ability to jam	Yes	Yes
Behavior of the attacker	Acts as legitimate as an AP in a WLAN	Mostly acts maliciously
Location of the Attacker	Near to victim or far away (2 miles)	Near the victim

same in WPA2 and WPA3 except for the new Dragonfly authentication. This new authentication is merely increasing the Wi-Fi passphrase entropy and would not be a concern for the MC-MitM attacker as he does not even require it. The PMF procedures are also the same in both WPA2 and WPA3 security protocols. Therefore, the MC-MitM attacker can follow the same practices described in Section 3.2 to acquire the MC-MitM position between an already connected WPA3 client and AP. Recently orchestrated FragAttacks are the fresh examples of MC-MitM attacks in WPA3 networks.

Recently, the WFA has incorporated certain defenses against MC-MitM in their WPA3-2020 updates (Stephen Orr, 2020). New defense mechanisms incorporated in WPA3 hamper spoofing attacks, including MC-MitM attacks materializing from outsiders to a great extent. That is, as long as the attacker does not have the Wi-Fi passphrase, he cannot perform MC-MitM attacks. However, these new defense mechanisms are optional features in the WPA3, meaning that an unpatched WPA3 device (WPA3 devices that only implement mandatory security requirements such as the new Dragonfly handshake) is always exposed to MC-MitM attackers. To what extent a significant problem still needs to be explored is how to defend against various insider MC-MitM attacks effectively. This can be a significant issue when the attacker has a Wi-Fi passphrase and can access a network that hosts multiple WPA2 and WPA3 devices. In Table 3, we highlight the current issues in Wi-Fi security protocols in view of MC-MitM attacks.

4. Recent MC-MitM enabled attacks in IEEE 802.11 networks and their impacts

In this section, we thoroughly review existing MC-MitM enabled attacks (attacks performed after acquiring the MitM position) towards WPA and WPA2 networks and examine whether any of these attacks can be possible in WPA3 networks. Our main aim is to study various vulnerabilities exploited and related impacts of MC-MitM attacks. To review the existing attacks, we follow the classification of MC-MitM attacks presented in section 3.3.

4.1. Multi-Channel MitM attacks powered by base variant

In their work (Vanhoef & Piessens, 2014), the MC-MitM position is devised for the first time to attack the WPA-TKIP encryption protocol. They demonstrate how to abuse TKIP when used as a group cipher, targeting multicast and broadcast frames towards clients in a WLAN. While attacking a specific client, the authors employ the MitM position to block all Message Integrity Code (MIC) failure reports from other clients connected with the AP. Blocking the MIC failure report is essential to suppress TKIP countermeasures (renewing group keys for reconnection) from the AP. Further, they demonstrate how to capture and decrypt client traffic using the already known Beck and Tews method while guessing some specific frames and eventually derive the corresponding MIC key of broadcast frames. Following the MIC key's derivation, they extend the attack targeting multiple wireless clients in a WLAN. Since this MitM attack mainly exploits the flaws associated with TKIP's Michael algorithm (Beck & Tews, 2009), it can be practical in every WPA-TKIP or WPA2-TKIP network. However, this attack is not possible against WPA3 networks as the WPA3 does not support TKIP (Cisco, 2021).

Table 3
Current issues in Wi-Fi security protocols related to MC-MitM attacks.

Protocol	Deauth /Dissassoc-Attacks	Outsider MC-MitM attacks	Insider MC-MitM attacks
WPA	Possible	Possible	Possible
WPA2	Possible	Possible	Possible
WPA2-PMF	Not Possible	Possible	Possible
WPA3	Not Possible	Possible with unpatched WPA3 devices	Possible even with patched WPA3 devices

A size-exposing attack has been proposed by (Goethem et al., 2016) for manipulating encrypted web traffic with the MC-MitM position while tricking the victim into sending requests and the forward frames to the real AP. This attack enables the authors to learn about the size of the resources (e.g., the size of the web packets) and then identify user web activities or websites visited. More precisely, they capture and manipulate encrypted (TKIP/CCMP) MAC layer frames of a specific TCP connection (target connection of the victim) to derive the exact size of the HTTP/S messages. The MC-MitM position helps the attacker to block unwanted background traffic (other than targeted TCP connection) to a victim and precisely calculate the size of the resources or packets accessed by him. Moreover, the MitM position manages retransmitted frames and reduces potential packet loss at the MAC layer. According to the authors, the size-exposing attack happens because the padding is never added while encrypting MAC layer frames, and no matter which encryption algorithm is used, the attacker can determine the length of encrypted plaintext in any Wi-Fi network. Therefore, such attacks are also possible in WPA3 networks.

(Vanhoef & Piessens, 2016) have presented some design flaws in random number generators (RNG) in several implementations. They illustrate how these flaws lead to predicting a group key so that an attacker can inject malicious wireless frames and potentially decrypt specific group traffic in WPA2 networks. To accomplish this, with the MC-MitM position, the attacker triggers security downgrade attacks by modifying beacons and probe responses to trick the victim into thinking that AP supports only TKIP instead of CCMP. This enables AP to start using RC4 (encryption algorithm of WPA-TKIP) for encrypting that communication session. The attacker exchanges the first two handshake messages between the AP and client with the MitM. When the AP accepts downgrade requests, it starts encrypting message 3 (containing the group key) with the RC4. The attacker then captures message 3 and recovers the group key exploiting the above-mentioned design flaws in RNG. Once the group key is derived, it enables the attacker to inject broadcast wireless packets and, in turn, decrypt all the Wi-Fi traffic.

Another security downgrade attack is presented by (Vanhoef et al., 2017). Here, with the MC-MitM position, the authors show how the attacker manipulates beacons and probe responses to trick the victim into thinking that AP supports only TKIP instead of CCMP even though both devices support CCMP. More concretely, the MitM attacker first relays messages 1 and 2 of a 4-way handshake during the attack and then blocks message 3 to hide RSNE details. Following this, the attacker sends a crafted message 1 to force the client to retransmit message 2, which will be forwarded to the AP. However, the AP wrongly interprets this message 2 as message 4 (vulnerability) and finishes the 4-way handshake. As a result, the client will connect to the AP and use TKIP as the selected cipher suite. Once accomplished, the authenticator starts encrypting frames using TKIP. As of now, the attacker can decrypt sensitive information by exploiting known vulnerabilities of RC4.

As mentioned before, since WPA3 does not support TKIP, the security downgrade attacks presented in (Vanhoef & Piessens, 2016) and (Vanhoef et al., 2017) cannot be possible in WPA3 networks.

In the mid of 2017, (Vanhoef & Piessens, 2017) have discovered severe key reinstallation vulnerabilities (nonces and replay counter reset during a session key installation) in 802.11 standards. Recall Section 3.4, where we have demonstrated the working principles of key reinstallation attacks. In practice, these vulnerabilities can be abused to decrypt TCP packets of a specific connection and then possibly hijack application layer (HTTP/S) traffic. It is also trivial for the attacker to hijack device control commands in IoT networks by replaying specific broadcast and multicast UDP packets. The KRACK was severe against TKIP and GCMP data confidentiality protocols as the attacker can even forge and inject malicious packets into Wi-Fi networks. Like 4-way handshake abuse, MC-MitM attackers can also abuse Group Key

handshake and Peer Key handshakes. Furthermore, in (Vanhoef & Piessens, 2018), which is the follow-up work of (Vanhoef & Piessens, 2017), they presented how KRACK can be performed on Tunneled Link Peer Key (TPK) handshake and Group Key handshake using WNM sleep mode frames. These KRACKs affect mobile device's roaming facilities and wireless direct connectivity features of smart TVs.

In Table 4, we examine different key reinstallation vulnerabilities (exploited using MC-MitM attacks) reported in 802.11 along with assigned CVE (Common Vulnerabilities and Exposures) identifiers from (NIST, 2021) and essential characteristics based on Common Vulnerabilities Scoring System. We highlight that leading vendor like Cisco and Google have assigned these vulnerabilities with a "high" score as millions of their Wi-Fi devices are highly affected.

4.2. Multi-Channel MitM attacks powered by improved variant

In (Vanhoef, 2017a), the author presented a serious implementation vulnerability in Android, Linux, and Chromium platforms, which could be effectively exploited using the improved variant. This vulnerability makes a Wi-Fi client install an all-zero-encryption key (encrypt frames with zero encryption key) instead of an actual encryption key during a 4-way handshake and enables the attacker to decrypt sensitive information effortlessly because of the absence of proper encryption during the data transmission. Nearly all implementations of Linux and Android 6.0 + platforms integrated with wpa_supplicant (v2.4 or above) are affected by this vulnerability and is exceptionally devastating against IoT devices, as most of them work on different flavors of Android or Linux platforms that internally use an affected version of wpa_supplicant. Another vulnerability enables an adversary to trick the Android clients (Chromium OS) into installing an already in-use group key. The attacker abuses the group key handshake to accomplish this task while distributing new group keys. This vulnerability critically affects most Wi-Fi devices as it enables an attacker to replay broadcast or multicast messages.

Recently in 2019, (Epia et al., 2019) has recreated the KRACK on Android devices and abused all-zero-encryption key vulnerability and traced useŕs private credentials from HTTP/S traffic. Fortunately, security patches are available for this vulnerability from WFA (Wi-Fi Alliance, 2017b).

Despite some KRACKs discussed in the previous section, in their follow-up paper, (Vanhoef & Piessens, 2018) presented several extensions of original KRACKs that are performed using the improved variant. In this paper, they mainly audited several available patches from WFA and some vendors and found that some are flawed and allow attacks in some instances. They also demonstrated an easier KRACK against a 4-way handshake by retransmitting an encrypted message 3 by abusing an AP's power-save functions, enabling them to attack unpatched Android devices. Most importantly, they showed a set of new key reinstallation techniques on 4-way and group-key handshake mechanism to bypass the WFA's official KRACK countermeasures by replaying the WNM (Wireless Network Management) sleep mode frames. These new KRACKs result in the encryption of data frames using an old session key so that the attacker can trivially decrypt the Wi-Fi traffic. The bypassing ability is significant-because it may enable the attacker to target even patched devices. However, the WFA has again released patches against bypassing vulnerabilities. Finally, some implementation-specific vulnerabilities are found in already patched Apple (macOS High Sierra 10.13.2) platforms that reuse station nonce values, enabling replaying handshake messages. On the other hand, Apple has patched this vulnerability.

According to (Vanhoef et al., 2018), the attacker in a WPA2 network can use the MC-MitM position several ways.

- SA query suppression can be performed whereby the MitM attacker can bypass the SA query mechanism when PMF is enabled. More specifically, after acquiring the MitM position, the attacker injects spoofed association or reassociation frames on behalf of an already connected client, which will trigger an SA query request from the AP. Consequently, the client sends back SA query responses to AP, but the MitM attacker instantly jams those responses. This causes resetting the connection (deletion of a current security association) at the AP side. The resetting of the connection makes AP unable to decrypt or recognize any packets from the client. Due to reset, the AP sends a deauthentication frame without any key (unprotected), which the PMF client would also ignore. Hereafter, the client enters into a deadlock situation as there is no way left for the client to reconnect with the AP. This attack can result in a stealthy DoS attack on PMF clients and can be possible in WPA3.
- While copying beacons, probe responses, and association frames, the MitM attacker can manipulate advertised capability and RSSI fields to deceive the clients.

Table 4
Impact analysis of key reinstallation vulnerabilities.

Assigned CVE	Handshake Details			Common Vulnerabilities and Exposures (CVSS VERSION 3.0)							Third Party Score	
	Type	Reinstall key	Attacker can retransmit	Base Score	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Confidentiality Index	Integrity Index	Cisco[1]	Google[2]
2017–13077	4-Way	PTK	Message 3	6.8 Medium	Adjacent	High	None	None	High	High	High	High
2017–13078	4-Way	GTK	Message 3	6.8 Medium	Adjacent	High	None	None	High	High	High	High
2017–13079	4-Way	IGTK	Message 3	6.8 Medium	Adjacent	High	None	None	None	High	High	High
2017–13080	Group Key	GTK	Grp. Msg. 1	6.8 Medium	Adjacent	High	None	None	None	High	High	High
2017–13081	Group Key	IGTK	Grp. Msg. 1	6.8 Medium	Adjacent	High	None	None	None	High	High	High
2017–13084	Peer Key	STK	Peer Msg. 2	6.8 Medium	Adjacent	High	None	None	High	High	High	High
2017–13087	Group Key	GTK	WNM Msgs	6.8 Medium	Adjacent	High	None	None	None	High	High	High
2017–13088	Group Key	IGTK	WNM Msgs	6.8 Medium	Adjacent	High	None	None	None	High	High	High
2017–13086	Peer Key	TPK	Peer Msg. 2	6.8 Medium	Adjacent	High	None	None	High	High	High	High

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171016-wpa.
[2] https://source.android.com/security/bulletin/2017–11-01.

- The MSDU (MAC Service Data Unit) can be manipulated to decrypt specific MAC level data. The last two attacks happen because respective fields in beacons are not cryptographically authenticated, which is also true for WPA3.

In their work, (Chi et al., 2020) show how MC-MitM attacks could be applied in real-world settings by attacking CBTC (Communication Based Train Control) systems. The CBTC network consists of several onboard WLAN-enabled controllers that exchange sensitive train control signals over protected Wi-Fi traffic to ensure safe and efficient trains' operation. Here in CBTC systems, the attacker is connected to WLAN. That is, the attacker is an insider (as he knows the legitimate Wi-Fi passphrase) and acquires MitM position to orchestrate operations such as block, delay, inject 802.11 frames. Most significantly, since the attacker knows the Wi-Fi passphrase, he could capture Wi-Fi frames between two legitimate devices and then directly decrypt, modify, and retransmit those frames on-the-fly. To decrypt frames, the attacker derives the session key PTK by using a passphrase (PMK), MAC address of end devices, and station nonces (Anonce and Snonce) as he gets all values except station nonces. However, he traces station nonces from a subsequent 4-way handshake forced by sending forged dissociation frames to the victim. In this way, an insider MC-MitM attacker hijacks other device's communication. This attack shows the power of the MC-MitM attacker if he has the Wi-Fi passphrase in WPA2 networks. Finally, all these attacks result in redundant traction, service collapse, including emergency braking of trains. On the other hand, these attacks are not possible in WPA3 because PMK is independent of the Wi-Fi passphrase.

In the middle of May 2021, Vanhoef discovered new design flaws related to aggregation and fragmentation features in the 802.11 standards that affect every Wi-Fi device, including the devices supporting WPA3 (Vanhoef, 2021a). These vulnerabilities can be exploited using attacks dubbed as FragAttacks, which use the MC-MitM position to inject malicious packets and then obtain sensitive data from a protected Wi-Fi communication. Aggregation attacks, fragmentation mixed-key attacks, and fragmentation cache attacks are three major attacks exploiting the new design flaws in the standards (recall Section 3.5 where we illustrate the working of these attacks). In essence, the FragAttacks can be used to inject intentional packets and trick the victim into using a fake DNS server, intercept and obtain sensitive Wi-Fi communication, grab web browser cookies, or facilitate DoS attacks towards connected clients. Affected platforms or devices include, but are not limited to, macOS, Android, Linux, Windows, IoT devices, professional and home APs. Though the design flaws are serious, abusing them is not trivial in practice as they rely on some preconditions such as user interaction or rekeying.

In addition to the FragAttacks exploiting the design flaws, Vanhoef has discovered several implementation vulnerabilities due to the common programming mistakes on Wi-Fi devices. Some of them can be trivially exploited in combination with the design flaws and can be summarized as:

- Wi-Fi devices do not verify whether fragments of the same frame possess consecutive packet numbers. The attacker can abuse this vulnerability to mix fragments from different sources through fragmentation mixed key attacks.
- Wi-Fi devices process mixed plaintext (unencrypted) and encrypted fragments instead of accepting only encrypted fragments. This flaw allows the attacker to replace or inject plaintext instead of encrypted ones by launching aggregation or fragmentation cache attacks.
- Wi-Fi devices forward plaintext EAPOL handshake frames to other clients even when the devices are not authenticated with the AP. This is a widespread implementation flaw found in home APs (e.g., Asus and Linksys). The attacker can abuse this flaw to perform an aggregation attack or fragmentation cache attack.
- Wi-Fi devices that support TKIP do not check the authenticity of resembled frames. This enables the attacker to trigger fragmentation attacks to inject and likely decrypt the frames.

In Table 5, we assemble the aggregation or fragmentation vulnerabilities (exploited using the MC-MitM) with assigned CVE from (NIST, 2021). Since the FragAttacks affect almost every Wi-Fi device, WFA has released concerned patches. We congregate different MC-MitM attacks performed using the base and improved variants in Tables 6 and 7.

4.3. Challenges in the adoption of general protection mechanisms

In this subsection, we discuss the significant challenges in adopting security patches (against KRACK and FragAttacks) and PMF in reducing the impact of MC-MitM attacks.

4.3.1. Challenges in security patching

As it can be observed from Tables 6 and 7, the MC-MitM position was widely used to trigger attacks like security downgrade attacks, DoS attacks, implementation-specific exploits, KRACK, and including the latest FragAttacks towards the protected Wi-Fi traffic. Fig. 15 shows the statistics of analyzed MC-MitM enabled attacks.

Amidst different attacks, the key reinstallation attacks and FragAttacks are most significant, which provide multiple ways to launch MC-MitM attacks due to the critical design flaws in the core handshake mechanisms and aggregation or fragmentation features of 802.11 standard. Since these attacks exploit flaws in the 802.11 standards, there is a high risk to every Wi-Fi device if the respective vendors have correctly implemented those standards. On the other hand, the WFA and affected vendors have released corresponding patches to prevent KRACK or FragAttacks. However, the available patches can only be applied to robust wireless clients (e.g., desktops, laptops, smartphones, professional routers) with provision for managing software or firmware patches in a much more hassle-free manner. Affected devices include millions of Wi-Fi devices connected to the Internet of Things (IoT) networks. Patching security vulnerabilities of key reinstallation, aggregation, or fragmentation can be challenging for several reasons, as discussed below.

4.3.1.1. Lack of security patches. IoT devices might most likely miss security patches against KRACK or FragAttacks due to insufficient patch support from respective vendors or companies. This is mainly because IoT companies release their devices, delivering seamless and hassle-free connectivity services at minimum cost, and adding continuous support increases the costs of deployment and maintenance. Additionally, to apply key reinstallation patches successfully, an IoT device requires an update of its underlying firmware and patches from the affected chip vendors (chip partners) that must be applied on devices' firmware patches (WILBUR, 2017). This requirement brings massive responsibility for device vendors because they must first receive updates from corresponding chip partners to release their new firmware patches. The conundrum is that device vendors do not release their patches because of limited update support periods even though chip vendors release their patches, while the reverse scenario is also possible.

Furthermore, IoT companies always go for dynamic changes for incorporating new services in their device to grasp the fast-paced growth of the Internet of Things markets. Thus, updates may not be available to devices as they neglect older devices or those devices with no sufficient market profit. Of great concern is that often vendors do not release patches even if responsible authorities notified them. For example, according to the CERT coordination center's vendor details shown in (CERT, 2017), we can see that only 17 % of notified device vendors have released patches during the coordinated patch release period during 2017. Fig. 16 shows those statistics from the vendor information page of CERT. Generally, well-known vendors such as Google, Microsoft, Apple,

Table 5
Impact analysis of aggregation and fragmentation vulnerabilities.

Assigned CVE	Attacker can perform	Common Vulnerabilities and Exposures (CVSS VERSION 3.0)							Third Party Score		
		Base Score	Attack Vector	Attack Complexity	Privileges Required	User Interaction	Confidentiality Index	Integrity Index	Cisco[1]	Aruba[2]	Synology[3]
2020–24588	Aggregation attack	3.5 Low	Adjacent	Low	None	Required	None	Low	Overall score is Medium, Individual score not available	Overall score is Medium, Individual score not available	Moderate
2020–24587	Fragmentation mixed key attack	2.6 Low	Adjacent	High	None	Required	Low	None			Moderate
2020–24586	Fragmentation cache attack	3.5 Low	Adjacent	Low	None	Required	Low	None			Moderate
2020–26146	Frag. mixed key/cache attack	5.3 Medium	Adjacent	High	None	None	None	High			Moderate
2020–26147	Agg. /Frag. attack	5.4 Medium	Adjacent	High	None	Required	Low	High			Moderate
2020–26139	Agg. /Frag. attack	5.3 Medium	Adjacent	High	None	None	None	High			Low
2020–26141	Frag. mixed key/cache attack	6.5 Medium	Adjacent	Low	None	None	None	Low			Moderate

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-faf-22epcEWu.
[2] https://www.arubanetworks.com/support-services/security-bulletins/#cat=3.
[3] https://www.synology.com/tr-tr/security/advisory/Synology_SA_21_20.

and other famous router manufacturers have released patches. However, patch release details of many vendors, including IoT manufacturers, are unavailable as per CERT.

Similarly, as shown in Fig. 17, the company Security Focus widely tested Wi-Fi devices (e.g., servers, operating systems, routers, Wi-Fi chips, IoT devices) in the year 2019 (Security Focus, 2019). They reported that 90 % of tested devices, including, but not limited to devices from Cisco, Aruba, Google, Microsoft, Intel, Apple, and Siemens, are vulnerable to key reinstallation attacks. Nearly all devices are affected here because, even if vendors release their new products or implementations, they generally ignore key reinstallation patches or test their new implementations against such vulnerabilities before commercializing them.

A recent experimental study (August 2020) presented by (Freudenreich et al., 2020) also concludes that several mobiles and IoT devices (around 65 % among tested) are still vulnerable to different types of key reinstallation attacks due to the unavailability of patches from respective device manufacturers.

All these statistics show that patching key reinstallation vulnerabilities or defending against KRACK is still a considerable dilemma even 4 years after their discovery. The main reason is, in reality, not every vendor releases patches responsibly for their new and old devices. So, it can be assumed that the same patching problems will continue for several years with the new FragAttacks. In other words, negligence in releasing patches makes most of the Wi-Fi devices in our home networks continue unpatched or exposed to MC-MitM enabled attacks.

On the other hand, although patches are available for MC-MitM enabled attacks, especially for KRACK and FragAttacks for WPA2 or WPA3 devices, there are no security patches for certain vulnerabilities related to WPA devices (e.g., (Vanhoef & Piessens, 2014), (Vanhoef et al., 2017), (Vanhoef & Piessens, 2016)). Even the available KRACK or FragAttacks security patches may not be applied on WPA devices because Wi-Fi Alliance deprecated TKIP in 2015 (Wi-Fi Alliance, 2015). WPA devices may be patched if the respective vendor specially develops patches for the vulnerabilities, but such actions are uncommon in practice. Unfortunately, several existing legacy Wi-Fi devices (e.g., smart TV, smart refrigerator, smart bulb), and mostly constrained IoT devices, are still working on TKIP to comply with their low-computing resources. Similarly, routers used in our home or office settings are still operating on TKIP/CCMP transition mode to avoid interoperability issues. The use of PMF is also not possible on WPA devices. A recent (Sept 2020) survey on Wi-Fi network issues conducted in (Reyes et al., 2020) critically shows that more than 50 % of analyzed devices employ WPA-TKIP. This is a critical condition where MC-MitM attackers will have multiple opportunities to potentially inflict damage on Wi-Fi environments by targeting those WPA-TKIP devices.

4.3.1.2. Patching difficulties. IoT device's realm experiences an enormous difficulty in dealing with updates, mainly due to applicability of patches on them. In many situations, IoT devices arrive with static programming or non-upgradable firmware models. This prevents such proprietary IoT devices from subsequent user-serviceable upgrading of the device or the Wi-Fi chip used in it (Chin & Xiong, 2018). Similarly, the security patches may not always comply with IoT device's firmware due to a mismatched vendor model, model of Wi-Fi chips, versions of hardware, or underlying operating systems. Fixing key reinstallation vulnerability is also risky because it likely damages the firmware of IoT devices. Another issue is the lack of I/O capabilities. For example, smart refrigerators, smart locks, window blinds, etc., often have no easily accessible user interfaces, and thus applying patches on them is difficult. Users also find difficulty in downloading patches as many IoT devices may not support over-the-air (OTA) updates (Lin & Bergmann, 2016). Additionally, to effectively defend against key reinstallation attacks, every device connected to the Wi-Fi network must be appropriately patched. Most clearly, every client and AP must be applied with patches, which is not usually feasible, especially when there are several heterogeneous devices in WLAN or home IoT settings. Updating only the affected router or client is not sufficient because even one unpatched device on a network can become a vulnerable component for MC-MitM attackers. Moreover, KRACK or FragAttack vulnerabilities have a set of more than ten security patches (Wi-Fi Alliance, 2017b, 2021) that must be applied separately on target devices. This makes the patching process more challenging, and thus, holistic patching is not practical, especially in IoT networks.

4.3.1.3. Lack of technical knowledge. While most people are aware of the key reinstallation vulnerabilities, they struggle or sometimes never perform patching due to the lack of substantial technical knowledge (Freudenreich et al., 2020). Sufficient device handling and installation skills are required for patching security flaws and bugs on Wi-Fi-capable devices. For devices like smartphones, this task is easy as it provides automatic push notifications and requires permission from the users. Similarly, if the vendor adequately maintains an IoT device by releasing

Table 6
Review of MC-MitM attacks (basic variant) in 802.11 networks.

Ref	Security protocol affected	Attack category	Purpose of MitM	Vulnerability exploited	Attack impacts	Attack on WPA2-PMF	Affected devices/ platforms	Countermeasures from authors	Patch's availability	Possible in WPA3?
(Vanhoef & Piessens, 2014)	WPA TKIP	DoS attack & Break encryption	To block MIC failure reports from clients and collect packets for processing.	Flawed MIC algorithm of TKIP	Inject and decrypt wireless broadcast traffic if WPA-TKIP is chosen.	Not Applicable	All Wi-Fi devices with WPA-TKIP.	AP should initiate TKIP countermeasures fastly.	Patches are not available as WFA deprecated TKIP. CCMP can be used instead.	No
(Goethem et al., 2016)	WPA/ WPA2 TKIP/ AES-CCMP	DoS attack	To block and forward wireless packets.	Padding is not added while encrypting MAC layer frames.	Reveal size of wireless frames, especially TCP packets and learn websites visited.	Not Applicable	Higher layer protocols such as TLS/HTTPS.	Virtual padding to avoid size information.	Not Available	Yes
(Vanhoef & Piessens, 2016)	WPA/ WPA2 TKIP/ AES-CCMP	Downgrade Attack on 4-way handshake	To forge and inject beacons supporting only TKIP and forward messages.	AP accepts WPA-TKIP, Design flaws in the random number.	Decrypt of specific Internet traffic in a WLAN.	Not Applicable	MediaTek (flawed RNG)Broadcom (depends on OS)	APs must disable support for TKIP	Patches are not available. CCMP can be used instead.	No
(Vanhoef et al., 2017)	WPA/ WPA2 TKIP/	Downgrade Attack on 4-way handshake	To advertise forged beacons supporting only TKIP and inject and forward messages.	APs accept TKIP cipher suite requests when it supports both TKIP and CCMP.	Decrypt wireless traffic exploiting known vulnerabilities of RC4.	Not Applicable	All Wi-Fi devices that use Wi-Fi chip from MediaTek, Telenet, and Broadcom.	RSNE parameters must be correctly verified.	Patches are not available. CCMP can be used instead.	No
(Vanhoef & Piessens, 2017)	WPA/ WPA2 TKIP/ AES-CCMP/ AES-GCMP	KRACK on 4-way handshake	To block message 4 collect, replay and message 3.	Wi-Fi devices reinstall old PTK due to resetting of nonce and/or replay counters.	Acquire sensitive information (e.g., passwords, chats, emails), hijack HTTPs, and inject malware.	Not Applicable	All Wi-Fi capable devices are affected. Found on MediaTek, macOS Sierra 10.12, wpa_supplicant v2.3–2.5	Devices must verify whether the generated session key is installed once, or under one session key, the nonce or replay counter is not reused.	WFA has released official patches. (Wi-Fi Alliance, 2017a)	No
		KRACK on 4-way handshake	To block message 4 collect, replay message 3.	Wi-Fi devices reinstall old GTK and IGTK due to resetting of nonce and/or replay counters.	Replay unicast, broadcast, and multicast frames. Impact IoT devices by replay of control commands.	Possible after acquiring the MitM	All Wi-Fi capable devices with MediaTek, macOS Sierra 10.12, wpa_supplicant v2.3-2.5, OpenBSD 6.1.			
		KRACK on Group-key handshake	To block message 2, collect, replay retransmitted messages.	Wi-Fi devices reinstall old GTK and IGTK due to resetting the replay counter.	Replay group messages between the AP and the client. Hijack IoT devices while broadcasting UDP commands.	Possible after acquiring the MitM	MediaTek, macOS Sierra 10.12, iOS 10.3.1, wpa_supplicant v2.3, 2.4, 2.5 and 2.6, Windows 10.			
(Vanhoef & Piessens, 2018)	WPA/ WPA2 TKIP/ AES-CCMP/ AES-GCMP	KRACK on TPK handshake	To collect, block, and replay PeerMessages	The 802.11z standard does not maintain a state machine of TPK handshake. Clients reuse nonces.	Decrypt and forge frames from smart TVs, IoT devices, and mobile phones Acquire personal sensitive information.	Not Applicable	All WPA2 devices that use wpa_supplicant versions 2.0 to 2.5.	After the first peer key message, clients shall install keys and not accept any messages after peer key message 3.	WFA has released official patches. (Wi-Fi Alliance, 2017a)	No
		KRACK on Group-key handshake	To block, collect, replay WNM-Sleep Mode response messages.	WNM clients reset the replay counter while reinstalling keys.	Replay WNM Sleep Mode frames.	Possible after acquiring the MitM	All Wi-Fi devices that support WNM Mode, macOS, iOS, and wpa_supplicant version 2.6.	APs shall follow the latest IGTK in EAPOL before entering WNM sleep mode frames.		

Table 7
Review of MC-MitM attacks (improved variant) in 802.11 networks.

Ref	Security protocol affected	Attack category	Purpose of MitM	Vulnerability exploited	Attack impacts	Attack on WPA2-PMF	Affected devices/ platforms	Countermeasures from authors	Patch's availability	Possible in WPA3?
(Vanhoef, 2017a)	WPA/ WPA2 TKIP/ AES-CCMP/ AES-GCMP	KRACK on 4-way handshake	To collect and retransmit message 3 multiple times to extend KRACK	Wi-Fi devices reinstall an all-zero session key	Decrypt client traffic from Android, Linux, and IoT devices.	Not Applicable	All Wi-Fi devices with Android 6.0 and above. wpa_supplicant v2.3–2.6, Chromium OS.	Wi-Fi chips must clear key in memory	WFA has released official patches	No
(Vanhoef & Piessens, 2018)	WPA/ WPA2 TKIP/ AES-CCMP/ AES-GCMP	KRACK on 4-way handshake	To block and collect message 4, inject forged sleep frames to the AP, and replay message 4.	Improper power-save management in APs.	Trigger KRACK at clients.	Not Applicable	All home routers (e.g., Cisco, Aerohive, Aruba, Ubiquity) with hostapd version 2.6, Linux, OpenBSD.	Devices shall track the replay counters. Integrity of power-save frames must be verified. Clients shall store a recent GTK & IGTK	WFA has released official patches. Wi-Fi Alliance has updated the standard (Dan Harkins and Jouni Malinen, 2017).	No
		KRACK on Group-key handshake	To block, collect the first two message 3 and forward to the client after WNM frames.	Wi-Fi devices reinstall an old GTK/IGTK.	Bypass WFÁs KRACK countermeasure.	Possible after acquiring the MitM				
		KRACK on 4-way handshake	To block and collect WNM-frames and broadcast frames from AP and retransmit them to the client.	Wi-Fi clients do not IGTK before going sleep mode.	Control Wi-Fi devices maliciously. Bypasses WFÁs KRACK countermeasure.	Possible after acquiring the MitM				
(Vanhoef et al., 2018)	Any	DoS on SA query procedure	To block SA-Query procedure from PMF enabled clients and send reassociation request to AP	PMF standard does not protect pre-authenticated management frames	PMF-enabled clients lose their connection from the AP.	Possible after acquiring the MitM	All PMF enabled Wi-Fi clients	Beacon protection (Vanhoef et al., 2020) may be used	Not Available	Yes
(Chi et al., 2020)	WPA/ WPA2 TKIP/ AES-CCMP/	DoS on CBTC systems (train control)	To collect, modify, and inject 802.11 frames between CBTC control systems.	Synchronization issues	Delayed or wrong train control, uncontrolled traction and service braking, interruption in train control, collision of two train bogies.	Not Applicable	WPA2 IoT sensors in CBTC	Not available	Not Available	No
(Epia et al., 2019)	WPA/ WPA2 TKIP/ AES-CCMP/	4-Way (KRACK)	To block, replay, and forge specific wireless frames to perform all-zero key reinstallation attacks.	Wi-Fi devices reinstall an all-zero session key	Recover the user details (e.g., username and password) when the victim visits certain websites using Android devices.	Not Applicable	Android 7.0 or above	Wi-Fi chips must clear key memory.	WFA has released official patches.	No
(Vanhoef, 2021a)	WPA/ WPA2/ WPA3/ TKIP/ CCMP/ GCMP	Frame aggregation attack Frame fragmenta-tion attack	To flip IPv4 packet into aggregated (A-MSDU) frame, To intercept, block, or forward specific fragments.	Aggregation flag in the frame header is not authenticated Lack of verification of fragments sent by different users, fragment cache not cleared.	Inject arbitrary packets, trick the client towards fake websites, mix malicious fragments, obtain or decrypt usés sensitive data.	Applicable	All Wi-Fi devices, Linux, Windows, macOS, iOS, IoT devices, routers (Cisco, Aruba, D -Link), NICs.	Ensure A-MSDU flag is authenticated in all frames. Fragments encrypted by different keys must not be processed, Cache must be cleared when (re) connection occurs.	WFA has released official patches. (Wi-Fi Alliance, 2021)	Yes. Attack reported on devices including WPA3.

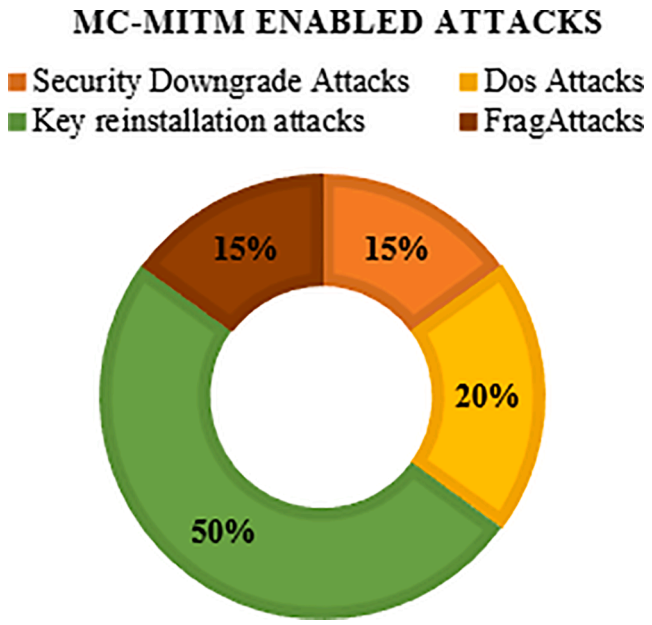


Fig. 15. Statistics of MC-MitM enabled attacks.

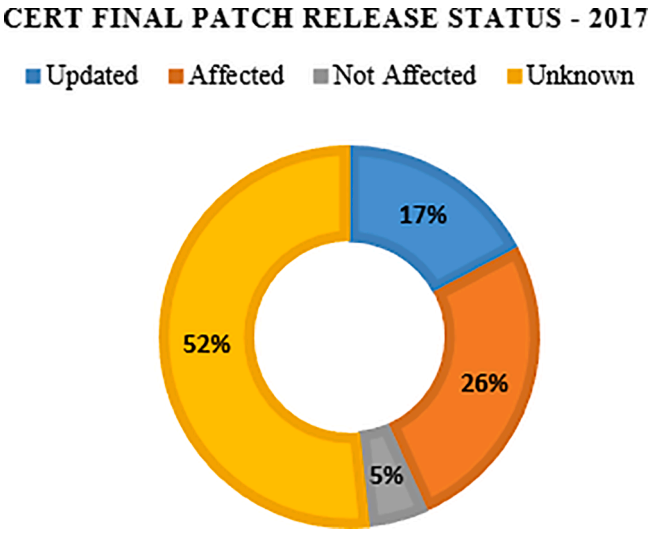


Fig. 16. Statistics of KRACK patch release by CERT.

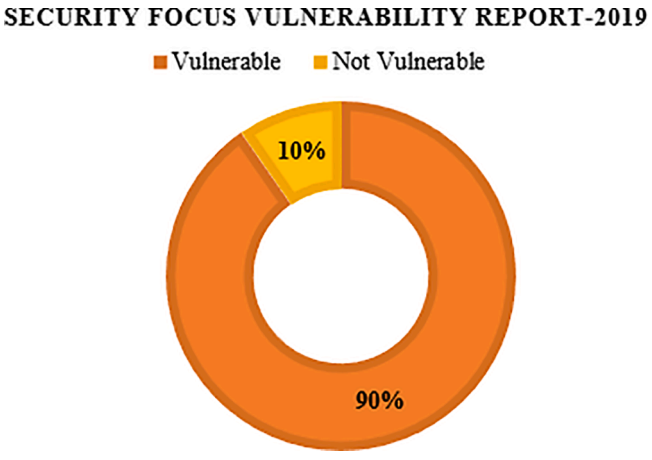


Fig. 17. Statistics of KRACK patch release by Security Focus.

patches, the user can apply the firmware patches through the connected mobile application. Patching some IoT devices (e.g., Raspberry Pi) is also difficult for common people as they need to download firmware according to the kernel version and then use specific Linux commands to apply the firmware patches. To apply patches on the APs, the user has to download firmware images of their router using its model number and firmware version. Then through the router web interface, he has to apply firmware upgrade by selecting the corresponding firmware images if the router does not provide automatic firmware update provisions. Additionally, users must be aware of rollback procedures in case of any firmware failures. In all cases, a substantial amount of technical knowledge is required.

4.3.2. Challenges in adopting PMF

Generally, PMF is used to defend against DoS attacks like deauthentication or disassociation attacks as part of MitM attacks from outsiders. Although PMF can resist these attacks, its adoption in existing WPA2 networks is quite challenging due to the following difficulties:

- PMF can defend DoS or MitM attacks only if every AP and client in a Wi-Fi network supports it. A PMF capable AP cannot admit a client that does not support PMF and vice versa. In personal Wi-Fi networks, the AP rarely supports the PMF and is available mostly if APs support 802.11n or 802.11ac standards. Generally, only high-end routers (e.g., Cisco) support PMF in enterprise networks (Cisco, 2020).
- It is generally difficult to enable PMF on existing Wi-Fi or IoT devices because proper software or firmware upgrade is required not just for an AP but also for every client (Cisco, 2017; CWNP, 2009). On the other hand, it is not possible to enable PMF unless device vendors support it.
- When PMF is enabled, some devices connect to the network for a short time and may suddenly get disconnected. On some devices, enabling PMF does not show an IP. Certain Wi-Fi clients do not support PMF if it runs on Wi-Fi version 4 or below (Cisco, 2020; Telstra Air, 2020).
- PMF may create many compatibility issues as it requires support from both the operating system (OS) and the Wi-Fi chip's driver used in devices (Cisco, 2017). For example, If OS supports, the chip's firmware may not always support 802.11w, or there will be no patches available for specific devices. It's generally unknown the devices or firmware versions that come with PMF.
- PMF cannot protect legacy Wi-Fi devices operating on TKIP to cope with their low-computing resources (CWNP, 2009; Reyes et al., 2020). Additionally, software patches cannot be applied on such devices as the WFA deprecated WPA-TKIP.
- PMF standard itself is vulnerable to key reinstallation attacks (CVE-2017–13081). Therefore, difficulties of KRACK security patching discussed in the previous section will also affect its use in real-world Wi-Fi applications.

On the other hand, PMF cannot defend against DoS attacks based on Wi-Fi jamming as well as rogue AP-based threats by spoofing the beacons (CWNP, 2009). This allows especially MC-MitM attackers to deceive WPA2 or WPA3 devices, even if PMF is enabled. Additionally, an insider MitM attacker can trigger deauthentication, disassociation attacks as he is authorized to access the network and so is the case with MC-MitM attackers.

4.4. MC-MitM attack scenarios in WPA3 networks and possible impacts

In this subsection, we analyze the possible impacts of MC-MitM attacks in WPA3 networks because of their ability to circumvent PMF protection. We create relevant attack scenarios where MC-MitM attackers can pose critical challenges in WPA3 networks.

4.4.1. Connection behavior of clients in WPA3 networks

This section depicts the connection behavior of the clients in WPA3 networks. As per Table 8, WPA3-Personal can be configured in two security modes: WPA3-Only mode and WPA3-Transition mode. In WPA3-Only mode, the AP accepts clients that support only WPA3 that use PMF by default. When WPA3-Transition mode is used, the AP accepts both WPA2 and WPA3 clients. Additionally, the AP can be set either as "required" or "enabled" modes in this configuration. In the "required" mode, the AP only accepts WPA2 or WPA3 clients with PMF, and in the "enabled" mode, the AP also accepts WPA2 clients without PMF. Important to note that WPA3 does not provide backward compatibility for WPA-TKIP clients.

4.4.2. MC-MitM attack scenarios in WPA3 networks

To deceive any device connected in a WPA3 network, the MC-MitM attacker can adopt either base or improved attack variants. Here, for the sake of analysis, we use MC-MitM improved variant attacks. However, the principal impact is the ability of MC-MitM attacks to circumvent PMF protection in acquiring the MitM position. Further, the following are the two different WPA3 attack scenarios, which amplify the impact of attacks.

4.4.2.1. WPA3-Only mode attack scenario and impacts. As depicted in Fig. 18, the MC-MitM attacker can target any of the WPA3 clients in the attack scenario. Once the attacker deceives a WPA3 client, he can block or modify any frames between the end devices and induce different kinds of FragAttacks (Vanhoef, 2021a). He can also perform DoS attacks such as SA query suppression and eventually disconnect the WPA3 client from the legitimate network. Size exposing attacks (Goethem et al., 2016) may also be effectively used to learn about the victim's private web traffic. Additionally, it is possible to modify advertised capabilities such as bitrates in beacons or probe response to control data bandwidth. According to (MTROI, 2014), when the attacker gains access to a WPA3 network (insider attacker), he can also send authenticated channel switch announcements through protected action frames and steer clients to connect his rogue channel. However, the MC-MitM attacker cannot perform KRACK or other kinds of offline dictionary attacks on WPA3 networks.

4.4.2.2. WPA3-Transition mode attack scenario and impacts. In transition modes (required and enabled) of WPA3 shown in Figs. 19 and 20 respectively, both WPA2 and WPA3 clients share a common Wi-Fi passphrase. So, with these attack scenarios, the MC-MitM attacker may target a WPA2-PMF or regular WPA2 client and capture specific four-way handshake messages to perform dictionary attacks. If found, attackers can challenge WPA3 networks by retrieving the password. Attackers can also decrypt previously encrypted WPA2 sessions but not WPA3 sessions. Though these attacks do not require a MitM position, the MC-MitM would facilitate such attacks more efficiently. Furthermore, KRACK is possible on both WPA2-PMF and regular WPA2 devices. SA query suppression and FragAttacks can also be performed on any WPA2 or WPA3 devices. All these attacks can potentially challenge the security of WPA3 networks.

Table 8
Client connection behavior in WPA3 networks (Cisco, 2021).

Security mode	PMF	Connection behavior of the client		
		WPA2 Client	WPA2-PMF Client	WPA3 Client
WPA3-Only	Required	Cannot connect	Cannot connect	Connection Possible
WPA3-Transition	Required	Cannot connect	Connection Possible	Connection Possible
	Enabled	Connection Possible	Connection Possible	Connection Possible

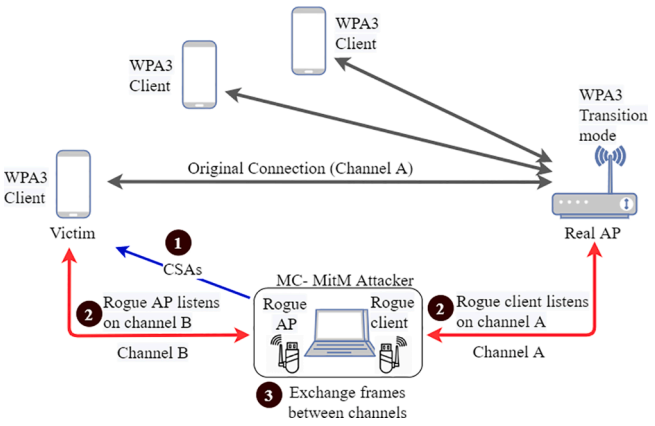


Fig. 18. WPA3-Only mode attack scenario.

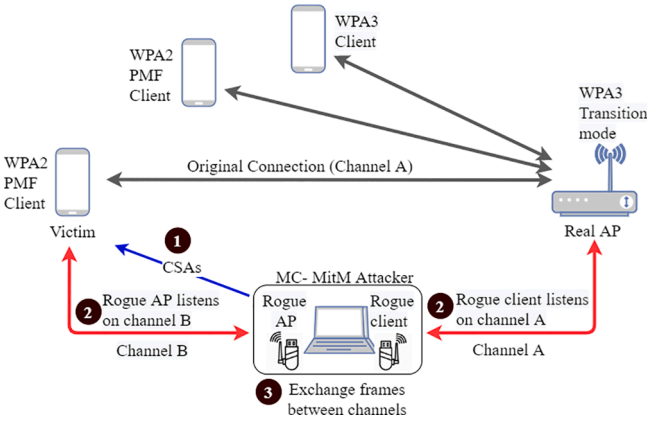


Fig. 19. WPA3-Transition mode-required attack scenario.

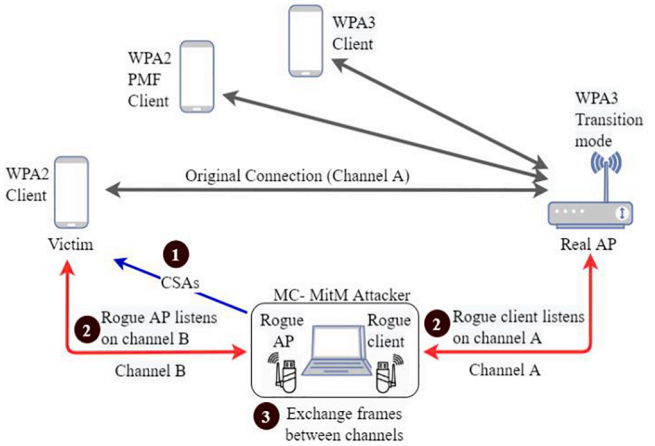


Fig. 20. WPA3-Transition mode-enabled attack scenario.

5. Multi-Channel MitM defense mechanisms

In this section, we analyse existing defense mechanisms for MC-MitM attacks. We also evaluate the feasibility of existing mechanisms for deploying in real-world IoT settings or environments.

5.1. Classifications of detection mechanisms

As shown in Tables 4 and 5 MC-MitM attacks have been a trend in attacking protected 802.11 networks since 2014. Based on the purpose

or application of the defense mechanisms, we classify them into two stages:

- **Stage 1 defense mechanisms**: This category focuses on defending against attackers before acquiring a MC-MitM position by recognizing real attack vectors, such as rogue devices, rogue channels, or spoofing channel switch announcements.
- **Stage 2 defense mechanisms**: This category focuses on defending against MC-MitM enabled attacks (e.g., KRACK, FragAttacks, DoS) or other attacks after acquiring a MitM position.

5.2. Analysis of stage 1 defense mechanisms

The first stage 1 defense mechanism is Operating Channel Validation (OCV), proposed by (Vanhoef et al., 2018), which cryptographically validate the parameters defining the operating channel between two wireless stations. They introduced a new Operating Channel Information (OCI) element (as an extension to the 802.11 standards) to be included in EAPOL frames and is verified during handshake processes (e.g., 4-way, group-key). In essence, on receiving handshake messages, the receiver verifies whether the OCI is present and the primary channel used for communication matches the one in the OCI of the sender. When a mismatch occurs, the OCV aborts the current handshake and prevents the attacker from acquiring the MC-MitM position. Besides, for preventing unprotected channel switch announcements through beacons or probe responses even when PMF is enabled, the authors proposed to include OCI in the SA query request-response messages of PMF.

To whatever extent the authors point out that the OCV still allows obtaining partial MitM (the attacker will be successful only if the AP sends CSAs). Here, the attacker tracks CSAs from the AP and jams them to keep the client stay on the old channel. He also captures and stores all frames from the client. Meanwhile, the attacker sends spoofed CSAs to the client before the AP starts disconnecting clients due to the SA query timeout. This will force the client to switch channels and complete the SA query. As of now, the attacker sends the previously stored frames to the AP and acquires the MitM. Similarly, it is also possible to acquire partial MitM (the attacker gains frames only from the client) by exploiting the specific bandwidth parameters that are not authenticated cryptographically. Though the impact is less, the possibility of partial MitM can allow the attacker to bypass the OCV. Additionally, insider attackers can send protected channel switch announcements through action frames and perform SA query suppression (jam specific SA query messages), causing the resetting of the client's connection or DoS.

In their work, (Vanhoef et al., 2020) have proposed a stage 1 defense mechanism known as beacon protection to defend against attacks abusing unprotected beacons. Their main aim was to prevent rogue AP-based attacks such as silencing stations, power constraints manipulation, possible partial MitM attacks in (Vanhoef et al., 2018), channel switch announcements in MC-MitM attacks, etc. They introduced an extra information element (IE) in every beacon so that the clients can verify it when connecting to an AP. To achieve this, they modify the Management Message Integrity Code Element (MME) of the Broadcast Integrity Protocol (BIP), which is a part of the PMF standard. In this mechanism, a Beacon Integrity Packet Number (BIPN) in the beacon is incremented after every transmission so as to detect spoofed or replayed beacons. Notably, a new group key called Beacon Integrity Group Temporal Key (BIGTK) will be distributed to every client when they connect and authenticate with an AP. This enables every client to generate the Message Integrity Code (MIC) to verify and authenticate beacons from legitimate AP and ignore any unauthorized ones without MME or invalid MIC value, thus avoiding the risk of rogue APs to an extent.

Beacon protection may effectively protect beacons or probe responses; however, it does not consider certain unauthenticated action frames with channel switch announcements that can be abused even if PMF is enabled. Moreover, to realize beacon protection in practice, every client needs to store a reference beacon frame before connecting to an AP to verify beacońs legitimacy using an already distributed group key (BIGTK). This requirement may be challenging to achieve, especially with constrained IoT devices having no access control or storage capabilities. Finally, the proposed mechanism does not block insider attackers. For example, suppose the MC-MitM attacker is connected to WLAN. In such scenarios, he can still introduce MC-MitM attacks (send CSA action frames to steer clients to his rogue channel) in a much easier manner as he is authorized to perform network operations. This may result in the hijacking of private communication of other users or devices inside homes or offices. (Chi et al., 2020) is a good example of such an insider MC-MitM attack.

We highlight that the aforementioned defense mechanisms, i.e., (Vanhoef et al., 2018) and (Vanhoef et al., 2020), are incorporated in 802.11 standards, and recently, in December 2020, the WFA included them in WPA3-2020 updates as optional features (Stephen Orr, 2020). Nonetheless, the effectiveness of both mechanisms depends heavily on stringent security conditions such as the support for PMF, especially to defend spoofing of channel switch announcements (CSAs) in WPA and WPA2 networks and the need for software or firmware patches for WPA, WPA2, as well as WPA3 devices (due to changes in handshake procedures).

In WPA3-2020 updates, the WFA also included another feature known as SAE-PK (Public Key) to uniquely identify APs in a WLAN during the connection establishment process based on ECC public key cryptography (Wi-Fi Alliance, 2020 § 6). This can be considered as a stage 1 defense as it prevents insider attackers from setting up rogue AP and performing MitM attacks. To implement SAE-PK, the network administrator generates a passphrase that acts as a fingerprint of the legitimate AP with which a client can connect to protected Wi-Fi (private or public) networks. SAE-PK authentication is an extension of regular SAE with an additional confirm message from the AP to the client consisting of the digital signature of the AṔs public key. As a result, the client can verify this digital signature using the public key. Therefore, even if the attacker knows the passphrase, he does not know the corresponding private key used to generate a valid digital signature. Consequently, the insider attacker would not be able to set up rogue AP and perform MitM operations. However, we conjecture that SAE-PK will not prevent MC-MitM attacks. This is mainly because rogue APs are identified only during the SAE-PK authentication phase or when the client connects to the AP for the first time. On the other hand, the MC-MitM attacker usually acquires a MitM position between an already connected client and the AP. He can also bypass the SAE authentication because, according to (Huawei, 2020), the WPA3 client uses an open authentication instead of an SAE authentication while reconnecting to an already authenticated or connected network.

Aware of the partial MitM based attacks in (Vanhoef et al., 2018), (Chatterjee et al., 2020) defined a stage 1 defense mechanism based on Physically Unclonable Functions (PUF) to prevent rogue AṔs actions during the MC-MitM attack. The PUF is a digital fingerprint that can act as a unique identifier for an electronic circuit board structure, which is very difficult to clone since no two devices can have similar PUF based identifiers. The basic idea is to generate a unique secret key from the AP's PUF signature and use it to mutually authenticate devices (the AP and client). A dedicated server (trusted third party) stores a PUF signature (a challenge-response value pair, aka CRP) of the AP in WLAN and assigns a secret key to every client. When a client wants to join a particular AP, it communicates with the server and proves its legitimacy using a secret key. Therefore, an attacker who does not know the PUF signatures of their rogue AP will not make the authentication successful, thereby blocking key reinstallations or related MC-MitM attacks using rogue APs. However, PUF based authentication itself is under threat of several kinds of MitM attacks (Babaei & Schiele, 2019).

In yet another stage 1 defense mechanism, (Gong et al., 2020) proposed an anomaly detection system for the Wi-Fi clients to find rogue AṔs actions during the MC-MitM attack. To find anomalies during the

connection establishment, they modify the source code of the wpa_supplicant (an open-source implementation for Wi-Fi clients) and install it on every Wi-Fi client in a WLAN. The modified wpa_supplicant verifies the uniqueness of a pair of BSSID (MAC address of AP) and ESSID (network name) when a client begins connecting to an AP. If they are not unique, the mechanism prevents the clients from connecting to that particular AP and alerts users. However, the effectiveness of the proposed anomaly detection depends only if the attacker uses reactive jamming that often produces less lag in receiving beacons from the legitimate AP so that the client can decide by comparing these beacons with that of a rogue AP. On the other hand, if the MC-MitM attacker uses a continuous jammer on the legitimate AṔs channel, AṔs signals or beacons will not be unavailable for the target client, making the detection difficult. Moreover, depending only on the uniqueness of the BSSID and ESSID pair will not be effective because there can be many situations with the same pairs of identities. For example, when the AP supports a dual-band connection, there can be chances to have the same pair of such identities.

Although the defense mechanisms by (Chatterjee et al., 2020) and (Gong et al., 2020) can harden MC-MitM attacks by analysing the uniqueness of the rogue AṔs identities, their practical adoption may be difficult in real-world scenarios. This is because, in the former one, PUF authentication can be implemented only on FPGA (Field Programmable Gate Array (FPGA) devices, and its extraction is impossible with proprietary or commercially available routers (Babaei & Schiele, 2019). Moreover, it requires a sophisticated software tool provided by the FPGA manufacturer for subsequent programming and configurations. In the latter one, installing wpa_supplicant may be possible on embedded devices (e.g., Raspberry Pi), but the installation can be challenging on proprietary Wi-Fi devices that use specific software/hardware from the vendors.

5.3. Analysis of stage 2 defense mechanisms

As soon as the reinstallation attacks reported in 2017, (Chin & Xiong, 2018) introduced a stage 2 defense mechanism known as KRACK-Cover in, which helps Wi-Fi end-users to detect the presence of key reinstallation attacks in a WLAN. The proposed mechanism first captures and analyses 802.11 MAC layer frames in the target network by using sensors followed by validating message configurations of frames. The mechanism then identifies respective packets transmitted from validated frames while executing the KRACK attack scripts, including retransmitted broadcast/multicast frames or retransmitted 4-way handshake messages targeting different clients. Finally, the system alerts the end-user with a warning message upon finding such dubious handshake messages present during executing KRACK attacks.

As a subsequent stage 2 defense to detect key reinstallation attempts, (Naitik et al., 2018) presented a detection mechanism for clients in a WLAN. Their system first collects 802.11 MAC layer frames and then extracts WPA key data from 4-way handshake frames to know nonces' value. This is followed by verifying whether duplicate message 3 (EAPOL frame) is present in the wireless network stream. The AP retransmits message 3 when the attacker blocks message 4 from the victim to the AP. Once duplicate message 3 is found, the detection mechanism generates alerts to the administrators. Closely related to (Naitik et al., 2018), Natital developed a KRACK attack detector using python scripts in (Securingsam, 2017). This script can be run on open-source APs (e.g., hostapd) rather than clients. It identifies any duplicate message 3 of the 4-way handshake in a particular WLAN and disconnects the suspected device, preventing it from sending any further sensitive data to the AP.

The defense mechanisms proposed by (Naitik et al., 2018) and (Securingsam, 2017) manage to identify retransmitted message 3 of the 4-way handshake during KRACK attacks executed using the MC-MitM position. As per the 802.11 standards, it is quite reasonable that an AP retransmits message 3 in many circumstances. For example, retransmission occurs due to network traffic congestion, or it may continue until the AP reaches its maximum retransmission limit. Therefore, blocking every retransmitted handshake message may result in frequent handshake failures. Instead, systems could have verified whether the same session key was reused in subsequent retransmissions.

In another work, (Abare & Garba, 2019) enhanced the stage-2 defense mechanism by (Naitik et al., 2018) and proposed prevention mechanisms to authenticate handshake messages against key reinstallation attacks. Here, to avoid forging WPA key data nonce values and retransmission of message 3 of the 4-way handshake, the proposed mechanism encrypts complete handshake messages, including nonce values Wi-Fi pre-shared key. While encrypting the handshake's first message (from AP to the client), they include a new Boolean value initialized to TRUE with other standard parameters. On receiving this, the client decrypts it and stores the Boolean value. The client then encrypts this Boolean value with the necessary parameters and forwards it to the AP in message 2. If the subsequent decryption is successful, the AP forwards message 3 with the client's respective MIC and otherwise, it aborts the handshake. After decrypting message 3, the client changes the Boolean value to FALSE before sending message 4 to the AP, which indicates that the pairwise key is installed once. Thus, by verifying the Boolean value, the client can detect and prevent the repeated installation of keys later when message 3 is retransmitted during key reinstallation attacks. Significant to note that this prevention mechanism mandates changes in the Wi-Fi standard.

A software-defined networking (SDN) based stage 2 defense mechanism is introduced by (Li et al., 2019) to defend key reinstallation attacks. The proposed mechanism consists of detection and prevention modules, and are hosted on the AP in a WLAN. The SDN controller parses and inspects each incoming Wi-Fi network frame to trace any duplicated message 3 of the 4-way handshake to detect attacks. Additionally, it verifies the nonce and replay counter value in the frame to ensure whether there is any key that has been reused. To prevent attacks, this mechanism requires the AP to be configured to work as an Open Flow Switch (OVS), which is a programmable network protocol for SDN environment. Once the SDN controller detects the attack, the prevention module updates attack details in the flow table's entries in the OVS and then redirects the attack traffic flows to a splash portal, a disk space to store attack traffic instead of forwarding it to the client.

Though defense mechanisms by (Abare & Garba, 2019) and (Li et al., 2019) provide detection and prevention of KRACK attacks, they focus only on basic KRACK attacks, i.e., retransmission of message 3 during a 4-way handshake. However, attackers can still instil other forms of KRACK attacks (e.g., group-key, peer-key, and WNM sleep mode frames) even with the above defense mechanisms.

(Cremers et al., 2020) have enhanced previous stage 2 defense mechanisms by developing completely new handshake protocols for preventing different forms of key reinstallation attacks. These protocols identify the nonce-reuse weaknesses of underlying cryptographic algorithms, thereby improving the security of handshake mechanisms in 802.11 standards, and are basically security patches that manage the nonce and replay counter reuses 4-way handshake, group key handshake, WNM sleep mode, etc. They also claim that their protocols can defend against key reinstallation attacks even in the absence of previous stage 1 defense mechanisms. Another formal model proposal can be presented in (Singh et al., 2020) that prevents different forms of KRACK and also defends against cipher suite downgrade attacks on APs. However, there is no evidence that these formal models are tested in real-world attack scenarios.

Traditional Intrusion Detection Systems like SNORT (Marty Roesch, 2021) released rules for detecting KRACK attacks in 2018 (SNORT, 2018). We consider SNORT as a post-attack defense mechanism since it identifies KRACK attacks triggered after acquiring the MC-MitM position. SNORT rules filter and detect malicious network packets with specific contents (e.g., Dot11, RadioTap, and FCfield) that may occur while running KRACK attack scripts. These filtering contents are key

components of the KRACK python script and Scapy (a packet manipulation tool) utilities. However, the contents used by SNORT rules for detecting or matching KRACK can even be present in typical WLAN packets or scripts of other attacks developed using Scapy. Hence, employing SNORT with this specific rule may be ineffective or generate false alarms.

5.4. Technical feasibility analysis of MC- MitM defense mechanisms

In this subsection, we define specific qualitative metrics to evaluate the technical feasibility of implementing stage 1 and stage 2 defense mechanisms against MC-MitM enabled attacks in real-world IoT environments. We assume that IoT environments host Wi-Fi supported constrained devices like smart lights, smart sensors (e.g., temperature, humidity, pressure), smart controllers (e.g., plugs, switches, curtain, door), smart appliances (e.g., thermostats, refrigerator, washing machine, oven) along with other robust devices such as home routers (APs), smartphones, laptops or computers.

5.4.1. Metrics used for technical feasibility analysis

We consider undermentioned metrics to evaluate the technical feasibility of existing defense mechanisms.

- **Changes in the Wi-Fi standard**: This metric indicates whether the proposed defense mechanism requires protocol changes in any of the existing Wi-Fi standards (802.11 or 802.11w).
- **Defense mechanism installation/compatibility:** This metric indicates whether the proposed defense mechanism requires the installation of new capabilities or expects their compatibility on every device (Wi-Fi client, AP) for successful implementation.
- **PMF requirements:** This metric indicates whether the proposed defense mechanism requires PMF on every device for its implementation.
- **Firmware updates:** This metric indicates whether the proposed defense mechanism requires firmware updates on every device to successfully execute new defense mechanisms or enable specific network configurations (e.g., PMF). Firmware updates are also required if the defense mechanism mandates changes in Wi-Fi standards.
- **Third-party software/hardware integration:** This metric indicates whether the proposed defense mechanism requires installing any third-party software (other than defense mechanism) or integrating additional hardware or storage requirements either with clients or on APs.
- **Computational complexity:** This metric indicates whether the proposed defense mechanism incurs computational overhead in terms of processing, memory requirements. We use relative measures as follows: high (when servers, routers, or computers/laptops with comparatively high processing power or storage used), moderate (when PMF or any other additional authentication or verification mechanism used), and low (no extra resources or additional software used).
- **Technical overhead:** This metric indicates whether the proposed defense mechanism expects substantial technical knowledge on standard users to set up or operate. We use relative measures as follows: high (users have to install or set up new defense mechanisms on devices or install any proprietary software, update software/firmware, or any other sophisticated task), moderate (users have to configure or enable PMF on router or clients, and low (no task other than executing/running mechanisms).

Based on the above metrics, we evaluate stage 1 and 2 defense mechanisms technical feasibility in Table 9.

5.4.2. Discussion on evaluation of technical feasibility analysis

As seen in Table 9, we highlight that every mechanism incurs high technical overhead on common people in several ways. We give much importance to this because, ultimately, the defense mechanisms will be managed by people without much technical knowledge. The existing defense mechanisms may be effective theoretically, in laboratory settings, or in simulation environments; however, their practicality is quite difficult in IoT environments. This is mainly because:

- Most defense mechanisms require Wi-Fi protocol standard changes that are hard to realize in practice, or the changes may take a long time for subsequent adoption by device vendors.
- Almost every defense mechanism is required to install or configure their new solutions or specific network settings either on every client, AP, or both. This requirement considerably increases the technical burden on users. Besides, it is hard to achieve that all devices, especially IoT devices, will have to be modified, updated, or replaced by new defense mechanisms. Also, any unsupported device can still act as a vulnerable entity for MC-MitM enabled attacks.
- Most stage 1 defense mechanisms depend entirely on PMF, but only some APs or router manufacturers support PMF. On the other hand, vendors rarely provide support for Wi-Fi clients. Enabling PMF might also require software/hardware updates on existing APs or clients. Additionally, PMF enforces advanced cipher suites or authentication mechanisms, which can be resource-intensive for IoT devices.
- Firmware updating is a significant task that needs adequate technical knowledge. While implementing existing defense mechanisms, firmware updates are required in most cases as they mandate either changes in Wi-Fi standards or installing their new mechanisms. However, this requirement may be easy on robust devices but hard to achieve on every IoT device.
- Integrating third-party software may be a difficult task in commercial or proprietary IoT environments as most of them may not always support it; moreover, such tasks are quite difficult for common people to set up themselves as the provision of technical support from IoT vendors is sometimes limited or non-existent. Besides, the said integration can increase the cost of maintenance, computational complexity, etc.

5.5. Summary

A significant concern stemming from the analysis of stage 1 defense mechanisms is the possibility of temporary MitM or insider MC-MitM attacks, especially with defense mechanisms included in WPA3. Although MC-defense mechanisms such as (Vanhoef et al., 2018) and (Vanhoef et al., 2020) are incorporated in 802.11 standards, they are not yet implemented in practice. On the other hand, most stage 2 defense mechanisms focus only on KRACK performed using the MC-MitM position. We could not find any stage 2 defense mechanisms in the literature related to MC-MitM enabled DoS attacks or the latest FragAttacks when writing this research paper. Similarly, the main takeaway from the feasibility analysis is that the existing defense mechanisms are not generalizable solutions to be practically implemented in IoT environments to effectively defend MC-MitM attacks. Further, we summarize the functionally, type of defense, advantages, and shortcomings of analysed stage-1 and stage-2 defense mechanisms, respectively, in Tables 10 and 11.

6. Research Problems, Challenges, and future research approaches

6.1. Research problems

The state-of-the-art research analysis on MC-MitM attacks motivates us to highlight two kinds of research problems. These include: (i) **Design deficiencies** of the standard. (ii) **Technical infeasibility** issues of existing defense mechanisms, especially in Wi-Fi environments hosting IoT and outdated devices.

Table 9
Technical feasibility analysis of Multi-Channel MitM defense mechanisms.

Metrics	Stage 1 defense mechanisms					Stage 2 defense mechanisms							
	(Vanhoef et al., 2018)	(Chatterjee et al., 2020)	(Vanhoef et al., 2020)	(Gong et al., 2020)	(Wi-Fi Alliance, 2020 § 6)	(Chin & Xiong, 2018)	(Naitik et al., 2018)	(Securingsam, 2017)	(Abare & Garba, 2019)	(Li et al., 2019)	(Cremers et al., 2020)	(Singh et al., 2020)	(SNORT, 2018)
Changes in the Wi-Fi standard	Required	Required	Required	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Required	Not Applicable	Required	Required	Not Applicable
Installation/ compatibility	Required on every device	Required on AP	Required on every device	Required on every client	Required on every device	Required on AP	Required on every client	Required on AP	Required on every device	Required on AP	Required on every device	Required on every device	Required on a client (pc/ laptop)
PMF requirements	Required on every device	Not Applicable	Required on every device	Not Applicable	Required on every device	This metric is not considered as it does not affect the implementation of stage 2 defense mechanisms							
Firmware updates	Required on every device	Required on AP	Required on every device	Required on every client	Required on every device	Not Applicable	Not Applicable	Not Applicable	Required on every device	Not Applicable	Required on every device	Required on every device	Not Applicable
Third-party software /hardware integration	Not Applicable	Required on every AP (Additional hardware)	Not Applicable	Not Applicable	Not Applicable	Required on every AP (Additional hardware)	Not Applicable	Not Applicable	Not Applicable	Required on AP (Additional SDN software and storage)	Not Applicable	Not Applicable	Not Applicable
Computational complexity	Moderate	High	Moderate	Moderate	Moderate	High	High	Moderate	Moderate	High	Moderate	Moderate	High
Technical overhead	High	High	High	High	High	High	High	High	High	High	High	High	High

As **design deficiencies** of the standard, we glean the fact that there are no related works currently protecting PMF clients from MC-MitM attacks as they are able to circumvent and trouble PMF protection in many ways. This is a significant open research problem concerning both new WPA2 and WPA3 devices as they now mandate PMF. According to our analysis presented in Section 4.4, MC-MitM attacks also impact WPA3 networks in all modes of the operation. Additionally, MC-MitM attacks are especially critical if the attacks originate from insiders (e.g., fragmentation cache attack). This may result in the hijacking of private communication of other users or devices inside homes or offices. None of the existing defense mechanisms can effectively handle such a problematic situation. However, it is of great importance, and researchers can analyse the real impact of MC-MitM attacks on WPA3 devices or especially when WPA3 operates in its transition mode with several WPA2 devices. Most importantly, future defense mechanisms must consider protecting both PMF-capable and incapable devices, thereby protecting them from MC-MitM attacks.

Regarding the **technical infeasibility**, according to what we have analysed and summarized in Section 5, successful deployment of the existing MC-MitM attack defense mechanisms is hard in practice from an IoT perspective. This is an important open research problem that needs imperative developments against MC-MitM attacks in IoT environments like smart homes. To the best of our knowledge, there are no studies that analyse and propose IoT-friendly, hassle-free (without much user intervention and changes in existing devices) defense mechanisms for protecting IoT environments from MC-MitM attacks. Affordable and effective defense mechanisms must be developed because commercial IoT devices are deployed everywhere, in homes, buildings, and offices to stay connected. Nevertheless, it is important to safeguard such devices as they carry lots of sensitive information. MC-MitM attackers can trivially trick or hijack these IoT devices to loot sensitive information as most of them sometimes practice no encryption, low encryption strength, insufficient randomness, or weak key generation mechanisms, and can perform any other malicious or unintended activities.

6.2. Research challenges

Our study on MC-MitM attacks and state of the art detection systems also urges us to showcase the following essential research challenges, which shall be considered to have an improved defense against these attacks.

Lack of sufficient backward compatibility is one of the major concerns of existing MC-MitM defense mechanisms. As we highlighted in Section 4.3.1.1, most of the currently deployed WPA2 routers in our home or office settings still support WPA-TKIP through its transition mode. This is mainly to avoid interoperability issues and provide long-term support for outdated or constrained devices that sometimes support only TKIP. On the other hand, security patches, PMF, and new defense mechanisms are not practical on IoT networks with outdated or constrained devices. Consumers purchase several devices and expect to work longer, which means that such devices will be in Wi-Fi networks for several years while remaining as relatively weak entities in view of MC-MitM attacks. None of the existing detection systems have some practical backward compatibility considerations to safeguard old devices in our smart environments.

Rogue AP detection as part of defending MC-MitM attacks can be challenging since the attacker cleverly spoofs almost every characteristic of the real AP and operates as legitimate in a WLAN (recall Section 3.6). As a result, such attackers can evade snooping-based rogue AP detection techniques by (Nikbakhsh et al., 2012). Usually, such detection strategies compare standard parameters of beacons, such as SSID, MAC addresses, channels, RSSI, sequence number, etc. However, the attacker can easily forge all these features if he knows them (Vanhoef et al., 2020). Communication channels can also be monitored or verified. But, blindly verifying the beacon's channel in a Wi-Fi medium may not be beneficial because there are many legitimate reasons for an AP to switch

Table 10
Summary of MC-MitM stage 1 defense mechanisms.

Ref	Functionality	Type of defense	Advantages	Shortcomings
(Vanhoef et al., 2018)	Cryptographically authenticate or validate operating channels of AP and client during a 4-way handshake.	Prevention (Cryptographic method)	+Prevents channel misuse, so implicitly blocks MC- MitM attacks triggered by both base and improved variants.+Provides backward compatibility using Operating Channel Validation Capable (OCVC) flag in RSN fields. +Protects channel switch announcements (CSA) using PMF. +Incorporated in draft of 802.11 standard.	-Mandates change in Wi-Fi standards. -Mandates use of PMF which may not be always achievable. -To take effect of OCI, both communicating parties must support it. -Partial MITM is possible by blocking CSAs. -Clients without OCI support remain vulnerable. -Mandates firmware changes on Wi-Fi chips, which may be impractical for IoT devices.
(Chatterjee et al., 2020)	A PUF based challenge-response procedure to counteract the threat of fake access points.	Prevention (Cryptographic method)	+Prevents fake access points, so implicitly blocks multi-channel MITM attacks triggered by both base and improved variants. +Every client uniquely identifies every access point in a WLAN.	-Mandates change in Wi-Fi standards-PUF signatures (instances) of every AP must be created and stored in a separate server. -Induces delay during 4-way handshake due to additional mutual authentication process. -High technical overhead on users. -Not suitable for commercial or proprietary IoT devices.
(Vanhoef et al., 2020)	Clients cryptographically authenticate beacons using an already distributed symmetric key from the AP.	Detection & Prevention (Cryptographic method)	+Prevents beacon spoofing. so implicitly blocks multi-channel MITM attacks triggered by both base and improved variants. +Detects and reports rogue AP. +Detects unauthenticated channel switch announcements (CSA) +Provides backward compatibility for older clients in identifying rogue APs. +Provides multiple BSSID beacon protection. +Incorporated in draft of 802.11 standard.	-Mandates change in Wi-Fi standard -Mandates use of PMF which may not be always achievable. -Does not protect action frames and may not fully confront MC-MitM attacks. -DoS attacks (flooding beacons) are inevitable. -Beacon protection does not protect insider forgeries. -Every client needs to store a reference beacon for verifying new beacons, which may be not ideal for IoT devices having constrained resources.
(Wi-Fi Alliance, 2020 § 6)	Clients identify the AP by verifying the digital signature of the APs public key and to block insider rogue APs	Prevention (Cryptographic method)	+Prevents insider rogue APs during the connection establishment. +Incorporated in WPA3 as an optional feature.	-MC-MitM attackers can bypass this method. -Additional communication overhead due to digital signature verification. -Useful only if every device supports this feature in WPA3.
(Gong et al., 2020)	Verify the anomalies in a pair of BSSID (MAC address of AP) and ESSID (Network name) when a client begins connecting to an AP.	Detection & Prevention (Anomaly detection Method)	+Detect rogue AP in a WLAN. +Alert the user. +Effective if the legitimate AP works on a specific channel.	-Requires changes in wpa_supplicant -Every client in WLAN requires to install the modified wpa-supplicant. -Ineffective if the AP operates on multiple channels, such as 2 GHz or 5 GHz. -Detection rate becomes lower when continuous jamming is used. -Integration may be difficult for proprietary IoT devices.

to different channels. Switching the channel is essential to avoid interference or noise in particular channels and is a dynamic action. Therefore, it may not be effective if we store an AP's channel to which a client was previously connected (Vanhoef & Piessens, 2014). Furthermore, since the attacker does not flood the network with beacons or probe requests, depending only on the frame arrival rate-based detection technique is not helpful. Additionally, when the MC-MitM attacker uses special reactive jamming while establishing the MitM position, it would be hard to detect by IDS systems (Gong et al., 2020). In the above scenarios, it may be challenging to correctly distinguish MC-MitM attacks.

6.3. Future research approaches

In light of the above research problems and challenges stemming from the analysis of MC-MitM attacks, we suggest that the best mitigation approach is a good intrusion detection strategy in line with the IoT environment's autonomous nature. We propose a signature-based intrusion detection system to detect MC-MitM attacks using specific traffic patterns or signatures during attacks. Our solution is to design a centralized, plug-and-play, and online passive monitoring system that can be easily integrated into Wi-Fi-based IoT environments without any modification to existing network settings or devices.

In order to outline this solution, we must first classify MC-MitM attack traffic into two stages. Stage 1 attack traffic appears first and consists of specific traffic on the legitimate channel that tricks the clients into selecting the attacker's channel in Wi-Fi networks. In the case of MC-MitM base variant attacks, a common stage 1 attack traffic is the constant jamming or reactive jamming. In MC-MitM improved variant attacks, the stage 1 attack traffic contains fake CSAs. Soon after the stage 1 attack traffic, once the MC-MitM position is reached, stage 2 attack traffic starts. Both MC-MitM attack variants exhibit identical stage 2 attack traffic. Thus, we propose a solution that uses stage 1 attack traffic to analyse different attack variants, and stage 2 traffic to confirm the presence of a potential MC-MitM attacker.

In the following sections, we briefly discuss the peculiarities of the aforementioned attack traffic and the specific metrics that might be used to identify it. We also present the design of our proposed signature-based intrusion detection system and its evaluation.

Table 11
Summary of MC-MitM stage 2 defense mechanisms.

Ref	Functionality	Type of defense	Advantages	Shortcomings
(Chin & Xiong, 2018)	Detect privacy evasive attacks using KRACK scripts in a WLAN.	Detection	+Detect key reinstallation attacks on clients. +End-users get alerts without installing additional softwares.	-Unable to detect KRACK other than the attack on 4-way handshake. -APs need integration of security modules.-Increased computational (storage) and communication costs. -High technical overhead on users. -Not adoptable for IoT networks.
(Naitik et al., 2018)	Detect key reinstallation attacks by identifying duplicated EAPOL message 3 of the 4-way handshake in a target WLAN.	Detection	+Detect reuse of nonces during 4-way handshake on clients. +End-users get alerts if the system detects duplicate packets.	-Unable to detect KRACK other than the attack on 4-way handshake. -Repeated handshake failures. -Roaming issues. -WPA key data can be forged. -Verifying WPA key data in every frame incur huge computational costs. -High technical overhead on users. -Difficult to integrate into IoT environments.
(Abare & Garba, 2019)	Prevent KRACK attacks by encrypting entire messages in a 4-way handshake by using a new Boolean value to track key installation.	Prevention (Cryptographic method)	+Detect and mitigate reuse of nonces and key reinstallation attacks during 4-way handshake on clients.	-Unable to detect KRACK other than the attack on 4-way handshake. -Mandates change in Wi-Fi standard. -Handshake failure can happen even without the presence of an adversary. -Increased computational costs due to additional calculation and verification of Boolean values during 4-way handshake. -Probable delay in 4-way handshake.
(Li et al., 2019)	Defend key reinstallation attacks using SDN.	Detection & Prevention	+Detect and mitigate reuse of nonces and key reinstallation attacks during 4-way handshake on clients.	-Unable to detect KRACK other than the attack on 4-way handshake. -APs needs integration of a SDN module.-Increased computational (storage) and communication costs. -Difficult to integrate into IoT environments.
(Cremers et al., 2020)	New formal models by properly using the nonces and replay counters of WPA2 handshake protocols.	Prevention (Cryptographic method)	+Detect key reinstallation attacks towards 4-way handshake, group key handshake, and WNM sleep mode. +Provides formal proof about the correctness of models.	-Requires additional security properties to be added to 802.11 standard. -Conceptual models and not tested in real world attack settings.
(Singh et al., 2020)	New formal models with additional security properties against various KRACK attacks.	Prevention (Cryptographic method)	+Detect key reinstallation attacks towards 4-way handshake, group key handshake, and WNM sleep mode. -Provides formal proof about the correctness of models.+Detects security downgrade attacks (TKIP/CCMP) .	-Requires additional security properties to be added to 802.11 standard. -Conceptual models and not tested in real world attack settings.
(SNORT, 2018)	Identifies KRACK packets using SNORT rules.	Detection	+Detect any forms of key reinstallation attacks packets.	-Generate false alarms as contents used for KRACK packets can be found in other normal packets.-Increased computational (storage) costs -High technical overhead on users.

6.3.1. MC-MitM attack signatures

6.3.1.1. Stage 1 attack traffic. When an attacker uses constant jamming against the AP's operating channel in an MC-MitM base variant attack, all traffic on that channel is blocked. As a result, no Wi-Fi frames are transmitted on a specific channel until the jamming is stopped (recall Section 3.3.1). This results in a sudden drop in beacon frame availability, which can be detected using metrics such as frame inter-arrival time (the time between the receiving of one frame and the reception of the next) and frame delivery ratio (ratio of the number of frames successfully delivered to the number of frames sent by the AP). When the attacker employs MC-MitM base variant attacks with reactive jamming, all beacons or probe responses on the AP's operating channel become malformed at a higher rate, which can be a good metric for detecting reactive jamming attacks.

In the case of MC-MitM improved variant attacks, CSAs can be used as a metric on the AP's operating channel, combined with checking if any transmissions still happen on the old channel after switching to the new one. This is because the legitimate AP in a WLAN doesn't know about the fake or spoofed CSAs, so it will keep sending beacons on its operating channel. In the case of genuine CSAs, on the other hand, the AP will only communicate through the new channel and stop communicating through the old one.

In order to define the signature of the stage 1 attack traffic, appropriate threshold values for FIAT, FDR, or malformed frame rate (for MC-MitM base variant attacks) and CSAs (for MC-MitM improved variant attacks) must be set based on empirical analysis of both benign and attack traffic scenarios during a specific time period.

6.3.1.2. Stage 2 attack traffic. The characteristic of stage 2 traffic is that it happens simultaneously on two different channels. To attract clients to the rogue channel, the MC-MitM begins retransmitting beacons acquired from the legitimate channel, resulting in beacons with the same SSID (network name) and BSSID (AP's MAC address) on two different channels at the same time. The client then detects these beacons and begins sending authentication frames, association frames, and 4-way handshake (EAPOL) frames. Meanwhile, the MC-MitM attacker gathers all frames from the originating channel and retransmits them to the other channel, allowing both end devices (the client and the AP) to negotiate the same session key (recall Section 3.2.1). Similarly, the attacker will

exchange data frames between the two different channels. We can distinguish various stages of stage 2 traffic by counting the number of frames (metric) that occur on two separate channels at the same time with the same SSID and BSSID during a specific period of time. Stage 2 traffic, like stage 1 attack traffic, should be empirically analysed in attack and benign traffic scenarios to determine acceptable threshold values.

6.3.2. Proposed solution

Fig. 21 depicts the high-level system architecture of our proposed signature-based intrusion detection system. It hosts the following units.

- Traffic interceptor unit captures and filters required wireless traffic.
- Device database unit automatically identifies and stores the MAC address of all the connected devices and delivers them to the MC-MitM detection unit.
- MC-MitM detection unit coordinates MC-MitM attack detection and recognizes the attack variant. It hosts three modules: the stage 1 and stage 2 traffic analyzer modules, which identify attack traffic for a specific period of time and record their various metrics, and the traffic collator module which collects those statuses from stage 1 and stage 2 and matches them against threshold values to identify MC-MitM attacks and its variants. Finally, this unit repeats the above procedure over the time to enforce continuous monitoring.
- Alert generator unit generates alerts in the event of MC-MitM attacks and logs details such as attack variants and identities of clients under attack.

6.3.3. Evaluation methodology

First, we must theoretically evaluate the viability of the thresholds for the proposed signature-based wireless intrusion detection, assuming that attack traffic is always distinct from benign traffic. We consider the different metrics discussed in the previous section to be the probability that a sample of wireless traffic is malicious, as computed by a statistical model, such that the values of the different metrics follow a normal distribution. In addition, wireless traffic must be analysed separately for benign and malicious scenarios, and all defined thresholds must fall within the first three standard deviations ($\mu \pm 3\sigma$), where μ is the mean and σ is the standard deviation. This ensures that the metric will be able to distinguish (99.7 percent) between benign and malicious traffic scenarios. Fig. 22 illustrates the distribution of metric values in benign and malicious traffic scenarios, where sample traffic with metric values greater than the threshold represents an attack and sample traffic with metric values less than the threshold represents benign traffic.

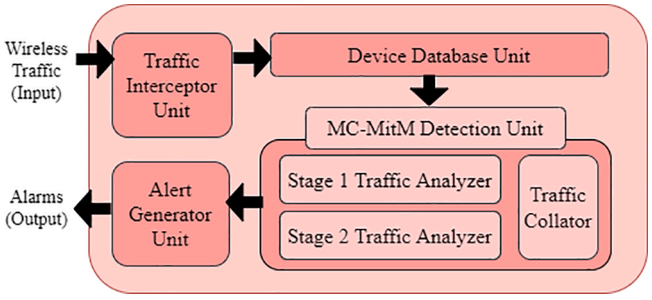


Fig. 21. System Architecture.

Unfortunately, in real-world scenarios, it is likely that the distributions of benign and malicious traffic will partially overlap, meaning that there will be a subset of traffic for which the system will not be able to predict whether it is benign or malicious based on the metric. Thus, thresholds must be examined to ensure that there is minimal overlap of distribution functions.. In particular, we should verify that our thresholds adhere to the stated rule ($\mu \pm 3\sigma$). The metrics whose thresholds do not meet the overlapping rule will be discarded from the attack signature.

In addition, we plan to evaluate our proposed system in a real-world Wi-Fi-based Internet of Things (IoT) environment, such as smart homes that contain a variety of heterogeneous devices, such as PCs, smart devices, and IoT sensors that use different Wi-Fi standards. More specifically, we intend to evaluate our proposed system in the real world by simulating various scenarios or use cases. These use cases will emphasize light/heavy traffic (network bandwidth) usage and detection from close/distant locations. We hypothesize that detection at a distant location with a heavy load will increase packet loss and produce poor detection results. This will lead us to the analysis of these variations in results in order to improve our proposed signature-based intrusion detection system, and using better fine-tuned thresholds or other detection strategies.

7. Conclusions

In this article, we have evaluated the capabilities of MC-MitM attacks and identified their distinct capabilities in manipulating protected Wi-Fi communications compared to traditional rogue AP MitM attacks. We have classified MC-MitM attacks, explored different kinds of related attacks in WPA, WPA2, WPA3, and analyzed their security impacts. Our analysis shows that MC-MitM attacks become more effective with the revelation of key reinstallation vulnerabilities, making such attackers decrypt communications from Wi-Fi devices unless appropriately patched. Though some patches are available, they do not apply to every

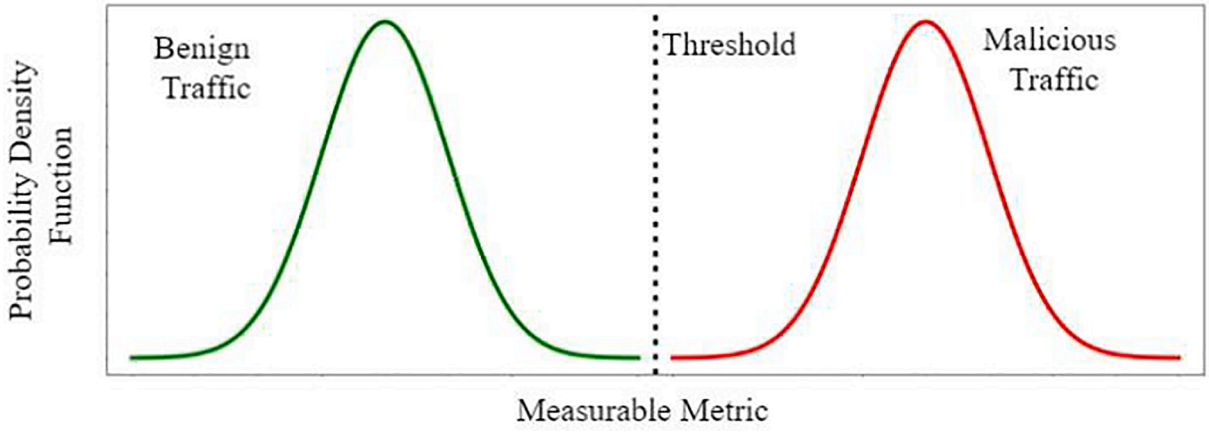


Fig. 22. Probability distribution of benign and malicious traffic.

Wi-Fi device. In this regard, we have identified significant security patching difficulties, especially on IoT devices. With the entry of recent FragAttacks, MC-MitM attacks become more widespread and practical to inject genuine packets into protected wireless networks and obtain usérs sensitive data. FragAttacks again brought huge challenges and a matter of security concern. Devices are likely vulnerable in the coming years due to the lack of proper implementation of Wi-Fi Alliance patches and adequate defense mechanisms. We can expect the same difficulties of KRACK patching with FragAttacks.

We identified that PMF could not be an adequate deterrent as it can be easily circumvented through MC-MitM attacks. Our studies shed light on the fact that MC-MitM attacks impact WPA3 networks in several ways due to their ability to circumvent PMF protection. We highlight this is a significant problem because WPA3 networks are evolving in our home and office environments. As far as MC-MitM defense is concerned, on the one hand, the existing mechanisms are not adequate as most of them allow some forms of insider MC-MitM attacks. On the other hand, MC-MitM attack defense remains an open research problem, especially from an IoT's perspective. We presented a technical feasibility analysis of the existing defense mechanisms, which uncovered that they are not flexible to be deployed in proprietary IoT networks consisting of constrained Wi-Fi-based IoT sensors and controllers.

This article gives the research community a view of MC-MitM attacks, their characteristics, and a fundamental understanding of the inner workings of various MC-MitM enabled attacks. It also highlights the importance of protecting Wi-Fi and IoT networks, especially when connected devices are working on different Wi-Fi protected access protocols and existing mechanisms cannot be practiced. To this end, we suggest developing lightweight and effective wireless intrusion detection systems for particularly defending against MC-MitM attacks in real Wi-Fi based IoT networks.

CRediT authorship contribution statement

Manesh Thankappan: Conceptualization, Methodology, Investigation, Writing – original draft, Visualization, Software. **Helena Rifà-Pous:** Conceptualization, Validation, Writing – review & editing, Supervision, Resources, Funding acquisition. **Carles Garrigues:** Conceptualization, Validation, Writing – review & editing, Supervision, Resources, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was partly funded by the Spanish Government through project **RTI2018-095094-B-C22** "**CONSENT**". We would also thank Mathy Vanhoef for his help by answering some of our queries and providing source codes related to MC-MitM attacks.

References

Abare, G., & Garba, E. J. (2019). A Proposed Model for Enhanced Security against Key Reinstallation Attack on Wireless Networks. 3, 21–27.

Alotaibi, B., & Elleithy, K. (2016). Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications, 90*(3), 1261–1290. https://doi.org/10.1007/s11277-016-3390-x

Louca, C., Peratikou, A., & Stavrou, S. (2021). 802.11 Man-in-the-Middle Attack Using Channel Switch Announcement. Springer International Publishing. doi: 10.1007/978-3-030-64758-2.

Babaei, A., & Schiele, G. (2019). Physical unclonable functions in the internet of things: State of the art and open challenges. *Sensors (Switzerland), 19*(14). https://doi.org/10.3390/s19143208

Beck, M., & Tews, E. (2009). Practical attacks against WEP and WPA. Proceedings of the 2nd ACM Conference on Wireless Network Security, WiSec'09, 79–85. doi: 10.1145/1514274.1514286.

Bertka, B. (2012). 802 . 11w Security : DoS Attacks and Vulnerability Controls. Infocom.

Burke, S. (2018). Wi-Fi Alliance introduces security enhancements. Retrieved from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements. Accessed 20 September 2020.

CERT. (2017). Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse. Retrieved from https://www.kb.cert.org/vuls/id/228519. Accessed 14 August 2020.

Chatterjee, U., Sadhukhan, R., Mukhopadhyay, D., Subhra Chakraborty, R., Mahata, D., & Prabhu, M. (2020). Stupify: A Hardware Countermeasure of KRACKs in WPA2 using Physically Unclonable Functions. The Web Conference 2020 - Companion of the World Wide Web Conference, WWW 2020, 217–221. doi: 10.1145/3366424.3383545.

Chi, M., Bu, B., Wang, H., Lv, Y., Yi, S., Yang, X., & Li, J., et al. (2020). Multi-channel man-in-the-middle attack against communication-based train control systems: Attack implementation and impact. In Lecture Notes in Electrical Engineering (Vol. 640). Springer Singapore. doi: 10.1007/978-981-15-2914-6_14.

Chin, T., & Xiong, K. (2018). KrackCover: A wireless security framework for covering KRACK attacks. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10874 LNCS (Issue 2). Springer International Publishing. doi: 10.1007/978-3-319-94268-1_60.

Cisco. (2017). 802.11w Deployment Guide- Chapter: 802.11w Protected Management Frames. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html Accessed 25 September 2020.

Cisco. (2020). Configure 802.11w Management Frame Protection on WLC. Retrieved from https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212576-configure-802-11w-management-frame-prote.html. Accessed 11 July 2020.

Cisco. (2021). WPA3 Encryption and Configuration Guide. Retrieved from https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide. Accessed 05 January 2021.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man in the Middle Attacks. *IEEE Communications Surveys and Tutorials, 18*(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

Cremers, C., Kiesl, B., Medinger, N., Symposium, U. S., Cremers, C., & Kiesl, B., et al. (2020). A Formal Analysis of IEEE 802.11's WPA2: Countering the Kracks Caused by Cracking the Counters. In 29th USENIX Security Symposium 20, 1-17.

CWNP. (2009). Wireless LAN Security and IEEE 802.11w. Retrieved from https://www.cwnp.com/wireless-lan-security-and-ieee-802-11w/ . Accessed 19 August 2020.

Epia Realpe, L. F., Parra, O. J. S., & Velandia, J. B. (2019). Use of KRACK Attack to Obtain Sensitive Information. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11005 LNCS, 270–276. doi: 10.1007/978-3-030-03101-5_22.

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, 4.1-4.14.

Freudenreich, J., Weidman, J., Grossklags, J., et al. (2020). Responding to KRACK: Wi-Fi Security Awareness in Private Households. In *IFIP Advances in Information and Communication Technology: Vol. 593 IFIPAI*. Springer International Publishing. https://doi.org/10.1007/978-3-030-57404-8_18.

Gong, S., Ochiai, H., & Esaki, H. (2020). Scan-Based Self Anomaly Detection: Client-Side Mitigation of Channel-Based Man-in-the-Middle Attacks against Wi-Fi. Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020, 1498–1503. doi: 10.1109/COMPSAC48688.2020.00-43.

Goethem V,T., Vanhoef, M., Piessens, F. (2016). Request and conquer: Exposing cross-origin resource size. Proceedings of the 25th USENIX Security Symposium, 447–462.

He, C., & Mitchell, J. C. (2004). Analysis of the 802.11i 4-Way Handshake. WiSE, 43–50.

Hiertz, G. R., Denteneer, D., Stibor, L., Zang, Y., Costa, X. P., Walke, B., et al. (2010). The IEEE 802.11 universe. *IEEE Communications Magazine, 48*(1), 62–70.

Huawei. (2020). Wireless Access Controller Configuration Guide. Retrieved from https://support.huawei.com/enterprise/en/doc/EDOC1100008282/b27702df/understanding-wlan-security-policies. Accessed 10 January 2021.

IEEE 802.11 Standard. (2012). Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications, ANSI/IEEE Std 802.11. https://ieeexplore.ieee.org/document/6178212.

Kaplanis, C. (2015). Detection and prevention of Man in the Middle attacks in Wi-Fi technology (Issue August). AALBORG UNIVERSITY.

Kohlios, C. P., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics (Switzerland), 7*(11). https://doi.org/10.3390/electronics7110284

Krischer, M. (2019). Securing the Wireless LAN. Retrieved from https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKEWN-2005.pdf Accessed 10 September 2020.

Li, Y., Serrano, M., Chin, T., Xiong, K., & Lin, J. (2019). A software-defined networking-based detection and mitigation approach against KRACK. ICETE 2019 - Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, 2 (Icete), 244–251. doi: 10.5220/0007926202440251.

Lin, H., & Bergmann, N. (2016). IoT privacy and security challenges for smart home environments. *Information, 7*(3), 44. https://doi.org/10.3390/info7030044

Lucas Woody. (2018). mitm-channel-based-package. Retrieved from https://pypi.org/project/mitm-channel-based/. Accessed 12 November 2020.
Marty Roesch. (2021). SNORT. Retrieved from https://www.snort.org/. Accessed 22 September 2020.
MTROI. (2014). Protected Management Frames (802.11w). Retrieved from https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w/. Accessed 25 September 2020.
Naitik, Lobo, R., Vernekar, P. S., & Shetty, V. G. (2018). Mitigation of Key Reinstallation Attack in WPA2 Wi-Fi networks by detection of Nonce Reuse. International Research Journal of Engineering and Technology, 05(05).
Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2012). A novel approach for rogue access point detection on the client-side. Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, 684–687. doi: 10.1109/WAINA.2012.108.
NIST. (2021). NATIONAL VULNERABILITY DATABASE. Retrieved from https://nvd.nist.gov/#. Accessed 15 May 2021.
Philipp Ebbecke (Wi-Fi Alliance). (2020). Protected Management Frames enhance Wi-Fi network security. Retrieved from https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security. Accessed 08 November 2020.
Reyes Moncayo, H. I., Malaver- Mendoza, L. D., Ochoa-Murillo, A. L., et al. (2020). Survey of the security risks of Wi-Fi networks based on the information elements of beacon and probe response frames. *Scientia et Technica, 25*(3), 351–357. https://doi.org/10.22517/23447214.23781
Roth, V., Polak, W., Turner, T., & Rieffel, E. (2008). Simple and effective defense against evil twin access points. In *WiSec'08: Proceedings of the 1st ACM Conference on Wireless Network Security* (pp. 220–225). https://doi.org/10.1145/1352533.1352569
Securingsam. (2017). KRACK Detector. Retrieved from https://github.com/securingsam/krackdetector. Accessed 13 August 2020.
Security Focus. (2019). WPA2 Key Reinstallation Multiple Security Weaknesses. Retrieved from https://www.securityfocus.com/bid/101274. Accessed 16 September 2020.
Singh, R. R., Moreira, J., Chothia, T., & Ryan, M. D. (2020). Modelling of 802.11 4-way handshake attacks and analysis of security properties. In *International workshop on security and trust management* (pp. 3–21). Cham: Springer.
SNORT. (2018). POLICY-OTHER WPA2 key reuse tool attempt. Retrieved from https://www.snort.org/rule_docs/1-44640. Accessed 11 November 2020.
Stephen Orr. (2020). Wi-Fi Alliance Wi-Fi Security Roadmap and WPA3 Updates. Retrieved from https://www.wi-fi.org/download.php?file=/sites/default/files/private/202012_Wi-Fi_Security_Roadmap_and_WPA3_Updates.pdf. Accessed 21 December 2020.
Telstra Air. (2020). WiFi issues due to Protected Management Frames. Retrieved from https://crowdsupport.telstra.com.au/t5/broadband-nbn/wifi-issues-due-to-protected-management-frames/ta-p/900478. Accessed 13 August 2020.
Vanhoef, M. (2015). Advanced Wi-Fi Attacks Using Commodity Hardware. Retrieved from https://github.com/vanhoefm/modwifi#constant-jamming. Accessed 14 September 2020.
Vanhoef, M. (2017a). Chromium Bug Tracker: WPA1/2 all-zero session key & key reinstallation attacks. Retrieved from https://bugs.chromium.org/p/chromium/issues/detail?id=743276. Accessed 26 August 2020.
Vanhoef, M. (2017b). Key Reinstallation Attacks- Breaking WPA2 by forcing nonce reuse. Retrieved from https://www.krackattacks.com/. Accessed 10 August 2020.
Vanhoef, M. (2018). KRACKing WPA2 and Mitigating Future Attacks. Retrieved from http://papers.mathyvanhoef.com/crypto-wac2018-slides.pdf. Accessed 15 October 2020.
Vanhoef, M. (2021a). Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. Proceedings of the 30th USENIX Security. https://papers.mathyvanhoef.com/usenix2021.pdf.
Vanhoef, M. (2021b). Performing aggregation attack. Retrieved from https://papers.mathyvanhoef.com/fragattacks-slides-amsdu.pdf. Accessed 14 May 2021.
Vanhoef, M. (2021c). FragAttacks: Fragmentation & Aggregation Attacks against Wi-Fi. Retrieved from https://papers.mathyvanhoef.com/fragattacks-slides-2021-03-8.pdf Accessed 15 May 2021.
Vanhoef, M., Adhikari, P., & Pöpper, C.(2020). Protecting wi-fi beacons from outsider forgeries. WiSec 2020 - Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 155–160. doi: 10.1145/3395351.3399442.
Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I., Piessens, F., et al. (2018). Operating channel validation: Preventing multi-channel man-in-the-middle attacks against protected wi-fi networks. In *WiSec 2018 - Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 34–39). https://doi.org/10.1145/3212480.3212493
Vanhoef, M., & Piessens, F. (2014). Advanced Wi-Fi attacks using commodity hardware. ACM International Conference Proceeding Series, 2014-Decem(December), 256–265. doi: 10.1145/2664243.2664260.
Vanhoef, M., & Piessens, F. (2016). Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. Proceedings of the 25th USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/vanhoef.
Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce Reuse in WPA2. Proceedings of the ACM Conference on Computer and Communications Security, 1313–1328. doi: 10.1145/3133956.3134027.
Vanhoef, M., & Piessens, F. (2018). Release The Kraken: New kracks in the 802.11 standard. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 299–314). https://doi.org/10.1145/3243734.3243807
Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. Proceedings - IEEE Symposium on Security and Privacy, 2020-May, 517–533. doi: 10.1109/SP40000.2020.00031.
Vanhoef, M., Schepers, D., Piessens, F., et al. (2017). Discovering logical vulnerabilities in the Wi-Fi handshake using model-based testing. In *ASIA CCS 2017 – Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security* (pp. 360–371). https://doi.org/10.1145/3052973.3053008
W3Techs. (2021). Usage statistics of HTTP Strict Transport Security for websites. Retrieved from https://w3techs.com/technologies/details/ce-hsts. Accessed 16 May 2021.
Wi-Fi Alliance. (2015). Technical Note Removal of TKIP from Wi-Fi Devices. Retrieved from https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Alliance_Technical_Note_TKIP_v1.0.pdf. Accessed 14 October 2020.
Wi-Fi Alliance. (2017a). KRACK Security Patches. Retrieved from https://www.wi-fi.org/security-update-october-2017. Accessed 04 September 2020.
Wi-Fi Alliance. (2017b). Security Update October 2017. Retrieved from https://w1.fi/security/2017-1/. Accessed 04 September 2020.
Wi-Fi Alliance. (2020). WPA3 Specification. Retrieved from https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf. Accessed 03 December 2020.
Wi-Fi Alliance. (2021). Security update – May 11, 2021. Retrieved from https://www.wi-fi.org/security-update-fragmentation. Accessed 15 May 2021.
WILBUR, P. (2017). KRACK IoT: How the Latest Widespread Wifi WPA2 Vulnerability is Affecting the Internet of Things. Retrieved from https://www.hologram.io/blog/krack-iot-how-the-latest-widespread-wifi-wpa2-vulnerability-is-affecting-the-internet-of-things. Accessed 05 May 2020.
Wright, Charles V., Fabian Monrose, G. M. M. (2009). IEEE Std 802.11w-2009 (Amendment 4)-Protected Management Frames. IEEE Computer Society. http://analog.nik.uni-obuda.hu/ParhuzamosProgramozasuHardver/03_GPGPU-Fejlesztes/02_RozsnyaiAndor (CUDA-SzD)/doc/wifi/802.11/802.11w-2009.pdf.
Yeahhub. (2018). Create A Fake AP With DNSMASQ And HOSTAPD. Retrieved from https://www.yeahhub.com/create-fake-ap-dnsmasq-hostapd-kali-linux. Accessed 28 December 2020.

3

Multi-Channel Man-in-the-Middle attacks against protected Wi-fi networks and their attack signatures

Multi-channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks and Their Attack Signatures

Manesh Thankappan[1(✉)], Helena Rifà-Pous[1,2], and Carles Garrigues[1,2]

[1] Estudis d'Informàtica Multimèdia i Telecomunicació, Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Barcelona, Spain
{mthankappan,hrifa,cgarrigueso}@uoc.edu

[2] Center for Cybersecurity Research of Catalonia (CYBERCAT), Barcelona, Spain

Abstract. Multi-Channel Man-in-the-Middle (MC-MitM) attack is an advanced form of MitM attack that can manipulate protected wireless communication between the Access Point (AP) and connected clients in a wireless network. Frontline MC-MitM attacks in recent years include Key Reinstallation Attacks (KRACK) reported in 2017 and the FragAttacks reported in 2021. Such attacks affected millions of wireless devices, particularly those associated with the Internet of Things (IoT) systems due to faulty implementations of the standard. Despite the fact that there are security updates available to defend against specific attacks, significant issue is that most of the IoT and Wi-Fi devices do not comply with them. Existing security mechanisms to combat MC-MitM attacks are unfeasible since they demand firmware upgrades on all network devices or use of complicated hardware and software for deployment. In this paper, we empirically develop lightweight attack signatures capable of passively and quickly identifying various MC-MitM attacks without altering any existing protocols or devices.

Keywords: WLAN · MitM · Wi-Fi · WPA · MitM · MC-MitM · KRACK · FragAttacks · IoT · attack signature

1 Introduction

WLANs (Wireless Local Area Networks) are prone to a wide array of cyberattacks. MitM attacks represent a critical threat to WLANs, which allows the attacker to listen in on, alter, or spoof either of the two parties. This type of attack typically involves using two wireless cards, one being associated with his own AP or legitimate AP, and the other acting like a rogue AP by spoofing the legitimate one. Wireless clients can connect such rogue APs through the built-in automatic access point choosing function. In a WLAN, there are typically two methods for carrying out MitM attacks.

The first method, which we mention as a "traditional rogue AP MitM attack," involves launching a rogue AP that deceives clients to associate with it using an already-known or familiar wireless password. In order to manipulate the encrypted communication

The original version of this chapter was revised: the word "faculty" has been corrected to "faulty". The correction to this chapter is available at https://doi.org/10.1007/978-3-031-39811-7_27

E. Mercier-Laurent et al. (Eds.): ICCCSP 2023, IFIP AICT 670, pp. 269–285, 2023.
https://doi.org/10.1007/978-3-031-39811-7_22

between the AP and victims, such traditional rogue AP attacks thus require the attacker to know the wireless password in advance. Traditional rogue AP MitM attacks are often done with tools like Fluxion [1] and WiFi-Pumpkin [2]. Furthermore, if the wireless password is unknown, the above tools are used to conduct MitM attacks against unprotected or open wireless traffic. The second method, on which we are focusing this research, is the Multi-Channel MitM attack [3]. The attack also uses two wireless cards, but they are on different channels and create a fake connection between the victim client and the legitimate AP. This allows the MC-MitM attack to tamper encrypted wireless communication between them on the fly without knowing a wireless password. In MC-MitM attacks, the legitimate AP is cloned on a new distinct channel. This lets the attacker to exchange beacon, probe response, and connection establishment (such as authentication, association and 4-way handshake) frames between both channels (i.e., new and operating channels) at the same time, so they communicate and manipulate subsequent data frames between the AP and victims. The attacker obtains the MC-MitM position by employing either unique jamming techniques (which are hereafter referred to as base variants) or channel switch announcement (which are referred to as improved variants) to trick the victims to direct to his channels.

The key reinstallation attack (KRACK) is the most impactful and popular base variant MC-MitM attack. KRACK exploits vulnerability in IEEE 802.11 standard's (e.g., WPA/2) 4-way handshake mechanisms [4]. An attacker can exploit these vulnerabilities to decode/decrypt wireless frames, particularly from Android or Linux devices that support WPA or WPA2. FragAttacks is a recent non-vendor-specific attack series performed using the MC-MitM [5]. With FragAttacks, the attacker exploits a set of authentication flaws in the fragmentation and aggregation procedures of the 802.11 standards by injecting frames into protected wireless networks for tricking the client into using a malicious web server, and then obtaining sensitive client information. Such exploitations also affect the WPA3 standard. Most notably, millions of wireless enabled devices are at risk of these non-vendor-specific vulnerabilities due to faulty implementations of the standard. In our paper [6], we provide an in-depth evaluation of capabilities of different MC-MitM attacks.

In response to KRACK and FragAttacks, the Wi-Fi Alliance released security patches. In spite of the existence of these patches, the main concern is that they cannot be applied to every wireless device, especially IoT device due to the issues such as resource limitations, deprecated security mechanisms, deceased device support duration. Over 75% of wireless devices remain vulnerable to the KRACK vulnerability even four years after its disclosure [7]. The FragAttacks once again posed significant security challenges for wireless devices and IoT systems. It is expected that devices will be vulnerable in the following years as a result of a lack of security fixes for FragAttacks.

Besides providing security patches, the Wi-Fi alliance mandated the use of PMF (Protected Management Frame) standard [8] to ensure wireless communication integrity protection, particularly against spoofed deauthentication and disassociation based MitM attacks. In contrast, MC-MitM attacks do not use deauthentication attacks, but instead make use of certain management frames (e.g., beacons or probe frames), which PMF does not protect, thus allowing attackers to circumvent the PMF. In order to protect sensitive communications over WLANs, perimeter security measures, such as firewalls

and VPNs, are commonly used. Firewalls and VPNs work at higher layers, so they cannot detect MC-MitM attacks that target individual wireless clients, as such attacks exploit weaknesses in the data link layer.

MC-MitM attacks pose a challenge because the attackers behave as normal as an AP in WLANs. While acquiring the MitM position, he does not flood the wireless by disassociation/deauthentication packets or perform any other suspicious actions. MC-MitM attackers create a particular type of jamming using cheap wireless dongles to take the MitM settings, which can be relatively difficult for existing intrusion detection systems to detect. [3, 9]. This is due to the fact that the MC-MitM attack emits noise signals arbitrarily while jamming, which could be wrongly treated as non-wireless devices operating in the same frequency range.

The above scenarios make it difficult to correctly differentiate between MC-MitM attacks. Researchers have proposed some security mechanisms [10, 11]. In general, these security mechanisms are designed to cryptographically authenticate wireless channels or beacons so as to detect potential intrusions. Furthermore, such security mechanisms can be employed only if every device belonging to a WLAN is compatible with them. Moreover, they are heavily dependent upon modified standards, especially PMF. This strict security requirement unfeasible in Wi-Fi networks, particularly IoT scenarios. In some security mechanisms [9], anomalies are identified using identities of AP, such as network name (SSID) and MAC address (BSSID). Nevertheless, such mechanisms are more expensive due to the need for sophisticated software or devices, as well as multiple protocol modifications. Our paper [6] provides a detailed feasibility study of existing defense mechanisms. Therefore, it is necessary to develop a mechanism with some prudent decision-making intelligence to detect MC-MitM attacks in real-time and be lightweight enough to be deployed in IoT environments. In this paper, we identify potential parameters to recognize different MC-MitM attack signatures and analyze the feasibility to deploy lightweight MC-MitM detection.

2 Background

In this section, we briefly describe the inner workings of different MC-MitM attacks.

2.1 MC-MitM Attack Setup

The primary goal of MC-MitM attacks is to get the MitM position between the targeted client and the AP while preserving the original security association, and then exchange and manipulate encrypted traffic between them.

Figure 1 demonstrate how the MC-MitM attacker clones end devices (the AP and the client) on opposing side channels in order to establish a fake connection between them.

To gain the MitM position, it is necessary to force the victim to switch to his channel by jamming or issuing channel switch announcement (CSA). An attacker forces the client by broadcasting legitimate AP beacons that have been collected through channel A. While receiving those beacon frames on channel B, a client determines that it is previously associated in accordance with the preferred network list (PNL) and thereby

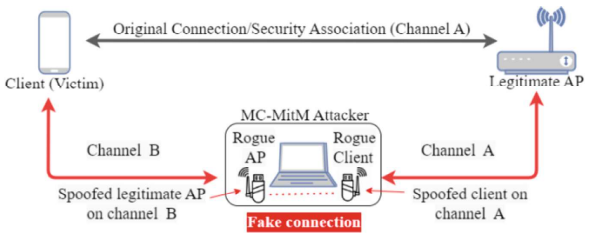


Fig. 1. MC-MitM attack setup

transmitting a probes on the chosen SSID. In response, the attacker sends (using rogue AP) a forged probe response targeting the victim on channel B, causing it to transmit authentication request frames on channel B. On the other hand, the rogue AP acquires such authentication request frames and retransmits them with the help of the rogue client on channel A. This results in the legitimate AP transmitting authentication response frames on channel A, whereas the rogue client acquires and retransmits them on channel B. (see Fig. 2a). Similarly, association frames are exchanged as depicted in Fig. 2b.

Following the exchange of association frames, the legitimate AP initiates a four-way handshake involving four EAPOL messages. Figure 2c illustrates how the MC-MitM attacker acquires the respective EAPOL messages from the source channel and retransmits them on the destination channel. While the attacker exchanges those handshake messages between two channels, they have a correct Message Integrity Check (MIC) when handled by the legitimate AP. Consequently, on their respective sides, the AP and client negotiate a similar and new session key (PTK). This session key is being used to encrypt data or communication between victim and the AP. As of now, the MC-MitM attacker subsequently hand over those encrypted data amid channels (see Fig. 3). This allows the attacker to reliably manipulate, i.e., blocking, delaying, modifying, injecting, replaying) encrypted frames amid end devices.

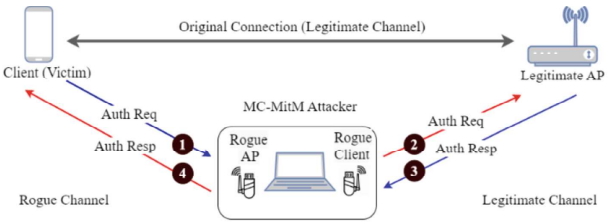
Moreover, the attacker uses the fake connection (see Fig. 1) to exchange encrypted wireless data in order to prevent the client and legitimate AP from communicating directly. The exchange of frames between channels is possible regardless of the authentication method with the AP. It is therefore possible to use MC-MitM attacks in both personal and enterprise Wi-Fi networks. Most importantly, it should be noted that the MC-MitM attack does not necessarily violate encryption protocols but rather makes use of specific vulnerabilities (e.g., in encryption or authentication) in IEEE 802.11 standards to obtain sensitive data.

Based on the tactics to force the client to change its channel, we categorize MC-MitM attacks into two variants: the base variant and the improved variant.

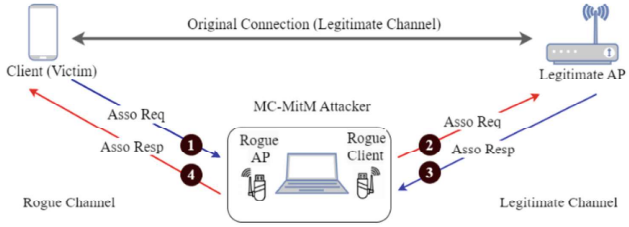
2.2 MC-MitM Base Variant Attack

Vanhoef and Piessens [3] introduced the MC-MitM base variant attack in 2014. Figure 4 demonstrates the working of a base variant MC-MitM attack.

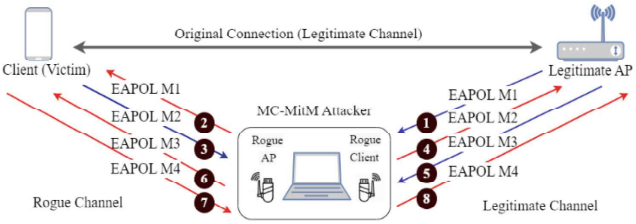
This variant uses two types of jamming techniques: constant jamming and reactive jamming. Constant jamming blocks traffic on a target channel entirely, whereas reactive



(a)



(b)



(c)

Fig. 2. Attacker exchanges: (a) authentication frames; (b) association frames; (c) EAPOL messages. The blue arrows indicate frames that are being acquired, and the red arrows indicate frames that are being retransmitted. Order of exchange is indicated by numbers on arrows. (Color figure online)

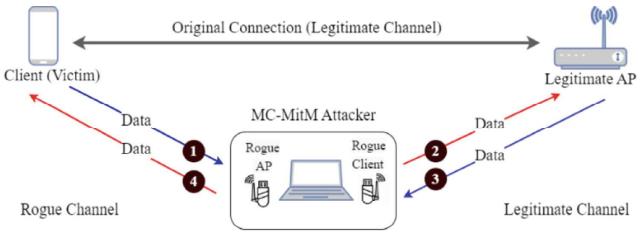


Fig. 3. Attacker exchanges the data frames. The blue arrows indicate data frames that are being acquired, and the red arrows indicate data frames that are being retransmitted. Order of exchange is indicated by numbers on arrows. (Color figure online)

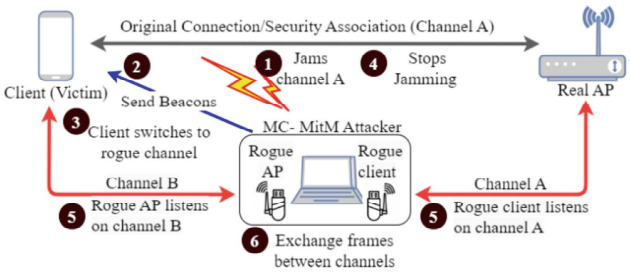


Fig. 4. MC-MitM base variant attack.

jamming jams specific frames (e.g., beacons or probe responses) by making them malformed. In the literature, [3, 4, 12, 13] are some MC-MitM-BV attacks using constant jamming, whereas [9] uses an MC-MitM using reactive jamming.

2.3 MC-MitM Improved Variant Attack

Vanhoef and Piessens [14] further proposed an improved variant of the MC-MitM attack using CSAs in 2018, which is more effective than the MC-MitM-BV attack. Figure 5 demonstrates the working of an improved variant MC-MitM attack. By using CSA, the cost and effort of jamming can be reduced significantly. In addition, only a few CSAs are required to execute the attack (four or five, as per the standards). CSAs are more effective since they represent AP's actions while receiving radar pulses that cannot be rejected by clients.[5, 15] are some notable examples of improved variant attacks**.**

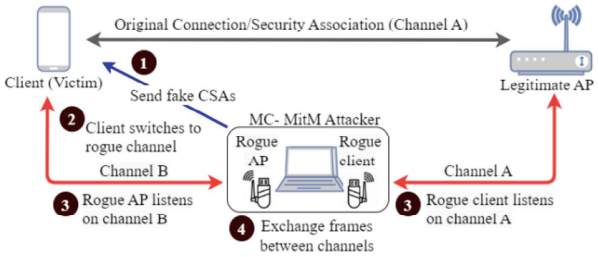


Fig. 5. MC-MitM improved variant attack.

In our paper [6], we extensively examined various MC-MitM attacks reported in the literature, as well as their potential impacts on Wi-Fi and IoT devices.

3 MC-MitM Attack Traffic Analysis

This section examines the peculiar network traffic behavior of MC-MitM attacks and corresponding network traffic behavior during normal or benign scenarios. Additionally, we identify possible metrics or parameters that change in relation to network traffic behavior when MC-MitM attacks occur.

We categorize MC-MitM attack traffic into two stages: stage 1 attack traffic and stage 2 attack traffic. At first, stage 1 attack traffic arrives on the operating or legitimate channel when the attacker tricks clients into selecting his channel. Stage 1 attack traffic in base variant attacks is typically constant or reactive jamming (see Sect. 2.2). Stage 1 attack traffic in improved variant is the arrival of fake CSAs (see Sect. 2.3). As soon as the attacker obtains the MitM position, stage 2 attack traffic arrives. Both variants of the MC-MitM attack generate similar stage 2 attack traffic. The following Tables 1 and 2 illustrate the peculiar behavior of stage 1 attack and stage 2 attack traffic, as well as the benign traffic behavior, and highlight metrics and parameters that can be used to identify different specific traffic behavior.

4 MC-MitM Attack Signature Creation

In this section, we design distinct attack signatures of MC-MitM through an empirical analysis about the attack traffic and benign traffic presented in the previous section. Furthermore, we identify appropriate threshold values for metrics to distinguish specific attack traffic.

4.1 Assumptions

We employ a threshold-based approach in order to passively identify signatures during MC-MitM attacks. Moreover, a threshold-based approach is cost effective and faster compared to artificial intelligence-based solutions. Furthermore, we design a signature or misuse-based detection, especially to identify different MC-MitM attack variants. By employing these attack signatures, we plan to propose a wireless intrusion detection system. Our solution is lightweight and suitable for plug-and-play installations. The solution must be simple to integrate into any Wi-Fi or IoT environment and ensure continuous protection against all kinds of MC-MitM threats without mandating any changes to network settings, protocols, or existing devices.

4.2 Reference Scenario

Figure 6 illustrates the setup in our university research lab for testing the suitability of specific metrics to identify attack signatures.

We set up three wireless clients and a transition-mode AP (D-Link AX router) to create WPA2 as well as WPA3 connections. We maintained a moderate network traffic by generating a maximum of 50 Mbps traffic using *iperf* tool during experiments. We implemented MC-MitM base variant attacks through the ModWifi tools [3] and MC-MitM improved variant attacks through multi-channel MitM [18]. Furthermore, we launched MC-MitM attacks alternatively against WPA2/WPA3 clients. We used Wireshark tool and TL-WN722N wireless dongles to collect client-AP communication (network traffic or wireless frames) through the MC-MitM position. Following sections analyze attack traffic over a specific time period, called the probe interval.

Table 1. Analysis of stage 1 network behavior while MC-MitM attacks

Signatures	Attack traffic behavior	Benign traffic behavior	Metrics
Constant jamming	Constant jamming indiscriminately jams all the traffic on a channel for a specific period of time, causing the clients to lose Wi-Fi connection from the legitimate AP	There should be no interruptions in a Wi-Fi connection, especially in receiving beacon traffic, as long as the client is in range of the legitimate AP	Wi-Fi frame inter arrival time (FIAT)[a] Wi-Fi frame delivery ratio (FDR)[b]. [17] employs above metrics to detect jamming attacks
Reactive Jamming	Reactive jamming causes instant malformation of all beacon traffic or probe response traffic for a specific period of time	Normally, malformation of frames occurs in Wi-Fi networks due to common issues such as incorrect frame reassembly. However, such a malformation frames occurs very rare in benign Wi-Fi networks	Malformed frame rate
Fake CSAs	CSAs usually occur near airports only if the DFS (Dynamic Frequency Selection) feature [19] is enabled in 5 GHz routers to avoid radar noise and is a rare event in household networks. CSAs will not occur in 2.4 GHz routers. When fake CSAs occur, there will be traffic (old and new or rogue channels)	When genuine CSAs occur, the legitimate AP begins communicating on the new channel and stops communicating on the old channel. This is because wireless networks or routers operate on one channel (operating channel) during its uptime	Number of CSAs

[a]Time elapsed between the reception of a frame and next frame
[b] Ratio of frames delivered to frames sent by the AP

4.3 Stage 1 Attack Traffic Signatures

In this section, we analyze stage 1 attack traffic signatures. We utilize these signatures as warnings of impending MC-MitM attacks and to differentiate between variants of these attacks. Additionally, we monitor the operating channel of the AP specifically this traffic.

Constant Jamming Attack Signature. As a first step, we connect the client and the access point wirelessly. Next, we conduct a probe interval of 60 s involving constant

Table 2. Analysis of stage 2 network behavior while MC-MitM attacks

Signatures	Attack traffic behavior	Benign traffic behavior	Metrics
Concurrent beacon traffic	This kind of traffic arrives simultaneously on two distinct channels with similar BSSID and SSID. This is because on the one hand, the attacker uses a rogue channel for transmitting beacons or probe responses, and in contrast, the legitimate AP, which is unaware of the attacker, will keep transmitting beacons on its operating channel	Such a traffic is impossible within WLANs. This is because wireless routers operate only on one channel to communicate with their clients during their uptime	Number of beacons or probe responses
Concurrent connection establishment traffic	This kind of traffic occurs simultaneously on two distinct channels with similar BSSID and SSID due to the exchange the authentication, association, and EAPOL frames between the operating or legitimate channel and the rogue channel for establishing the MitM position between the AP and victim (see Fig. 2)	Such a traffic is impossible within WLANs	Number of authentications, associations, or EAPOL frames
Concurrent data traffic	Following the concurrent connection establishment traffic, the attacker exchanges the encrypted data between the AP and the victim (see Fig. 3). This results in the occurrence of data frames simultaneously on two distinct channels with similar BSSID and SSID	Such a traffic is impossible within WLANs	Number of data frames

jamming for 30 s, followed by a 30-s network monitoring period. This experiment is repeated 50 times. For each probe interval, we compute FIAT values and FDR values (as explained in Table 1) of attack traffic and compare their values in terms of AVG (average) and SD (standard deviation) with that of benign traffic. We present the observed values of FIAT & FDR during different traffic scenarios in Table 3.

Table 3 illustrates how constant jamming affects values of FIAT as well as FDR. Therefore, in order to identify constant jamming attacks and warn against MC-MitM base variant attacks, we adjust the FIAT threshold to 2 ms(ms) and the FDR threshold to 50%.

Reactive Jamming Attack Signature. In our experiment, we observed reactive jamming attacks for a probe interval of five minutes. In this period, we mounted three periods of reactive jamming for 60 s, 100 s, and 150 s. We then captured the beacon and probe

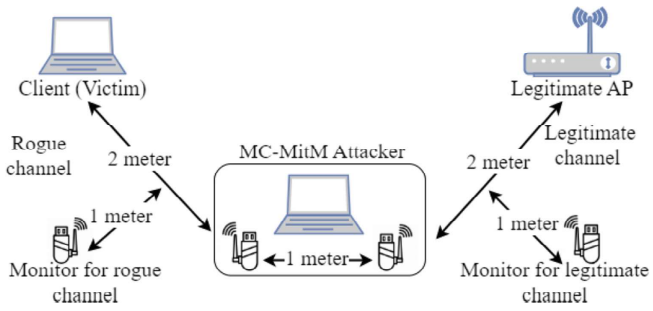


Fig. 6. Reference attack analysis scenario.

Table 3. Observed values of FIAT & FDR.

	FIAT (ms)			FDR (%)	
	AVG	SD		AVG	SD
Attack traffic	5	1.5		30	5.7
Benign traffic	0.1	0.02		90	1

response frames separately during each period and we discovered that more than 90% of the frames were malformed because of incorrect FCS, as shown in Fig. 7.

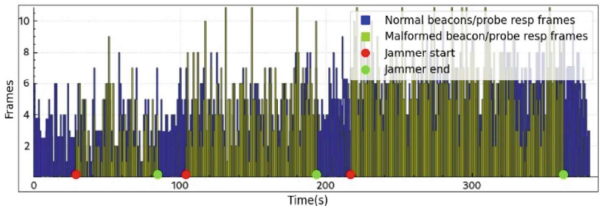


Fig. 7. Trace of network traffic when reactive jamming happens.

In contrast, after examining benign traffic for 15 min from the AP, we found only a negligible number of malformed frames (below 0.8%) belonging to beacons or probe responses, as shown in Fig. 8. As a result, malformed beacons or probe response frame occurring at a high rate (above 50%), particularly on the operating channel of the access point, may provide evidence of deliberate reactive jamming attempt. Consequently, we adjust the threshold of rate malformation to 50% so as to identify reactive jamming and warn against attacks involving the base variants of the MC-MitM.

CSA Attack Signature. Figure 9 illustrates the arrival of fake CSAs on the operating channel of the AP. It shows that the AP still transmits beacons on its operating channel despite CSAs occurred about 110 s. Ideally, this type of traffic should not occur with genuine CSAs since the AP begins communicating on the new channel after receiving

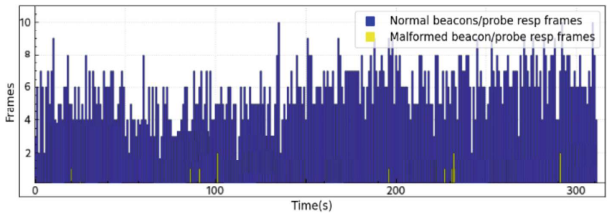


Fig. 8. Trace of benign traffic with malformed frames

CSAs. In contrast, during fake CSAs, the legitimate AP continues to send beacons on its operating channel because it does not know about the spoofed CSA.

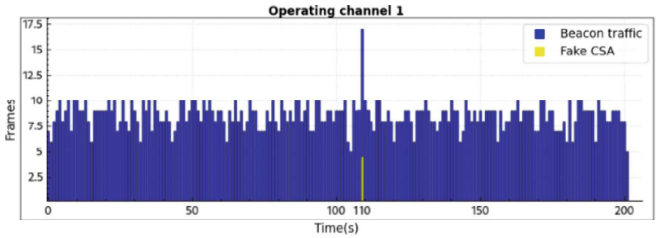
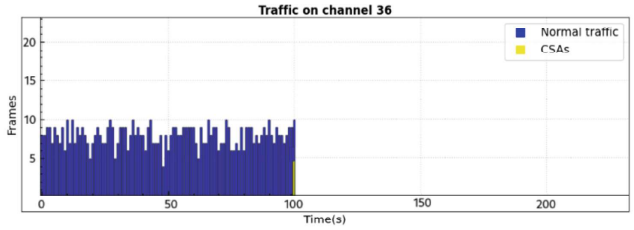


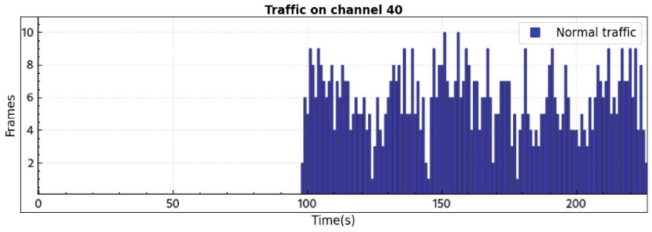
Fig. 9. Trace of network traffic during fake CSA attack.

In order to observe the benign traffic behavior in household networks during a genuine CSA, we switched channel of the AP from 36 to 40 by implementing a hostapd (software implementation of the access point) with the hostapd_cli interface. An example of a genuine channel switch is shown in Fig. 10. During this channel switch, we then simultaneously monitored channels 36 as well as 40 and found no traffic on operating channel 36 following the arrival of channel switch announcements about 100 s later. It should also be noted that the legitimate AP does not begin transmitting on channel 40 until the channel switch occurs, depicted in Fig. 10b.

Whenever a genuine channel switch occurs, the access point stops transmitting data on its current channel and transfers to the newly designated channel, and this can be used to distinguish whether CSAs are fake or not. As a result, to warn against possible improved variant attacks, we adjust the CSA threshold to 1 frame. DFS detectors can also be used to verify CSA occurrences [16]. In such detectors, radar pulses are recognized by advanced devices, which can increase the cost of detecting attacks. Instead, we consider that below mentioned attack signatures to detect fake CSAs. Furthermore, these signatures can potentially detect malicious CSAs irrespective of location, such as household networks or wireless networks near airports, where genuine CSAs can occur due to radar signals.



(a)



(b)

Fig. 10. Trace of benign traffic during a genuine CSA on (a) operating channel; (b) new channel.

4.4 Stage 2 Attack Traffic Signatures

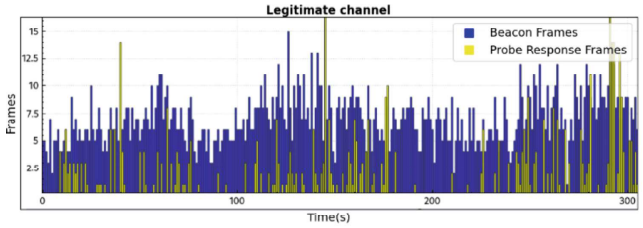
In this section, we develop stage 2 attack traffic signatures in order to identify and confirm the existence of deliberate MC-MitM attacks. To analyze traffic, we observe both operating (legitimate) and rogue channels simultaneously during a probe interval of about five minutes. During this time, MC-MitM attacks are launched in three periods (for about 60 to 100 s).

Concurrent Beacon Traffic Signature. Figure 11 shows a network trace of an attack consisting of beacons (or probe responses) on two distinct/separate wireless channels with the similar BSSID and SSID at the same time. Regarding corresponding investigation on benign traffic, we discovered no such beacon traffic on more than one channel belonging to similar frequency band within a WLAN.

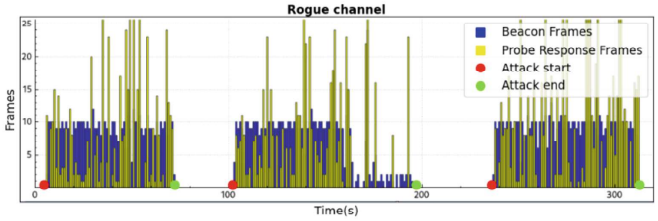
Thus, in conjunction with stage 1 attack traffic signature warnings, a sudden influx of beacon traffic on two distinct channels with similar BSSIDs and SSIDs can indicate MC-MitM activity within the WLAN. Therefore, we adjust the beacon (or probe response) threshold to 1 frame in order to quickly confirm this peculiar beacon traffic in a probe interval duration when MC-MitM attacks happen.

Concurrent Connection Establishment Traffic Signature. Figure 12 shows the network trace with multiple authentications, associations, and EAPOL messages/frames on two distinct channels with similar BSSID and SSID at the same time.

In the light of the aforementioned signatures, in conjunction with stage 1 attack traffic signature warnings, we confirm that these peculiar connection establishment traffic can potentially indicate the existence of MC-MitM attacks within a WLAN. Due to the frame exchange, if the MC-MitM attacker selects only one client/victim, there occurs

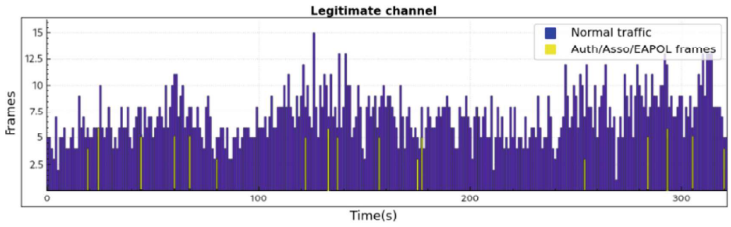


(a)

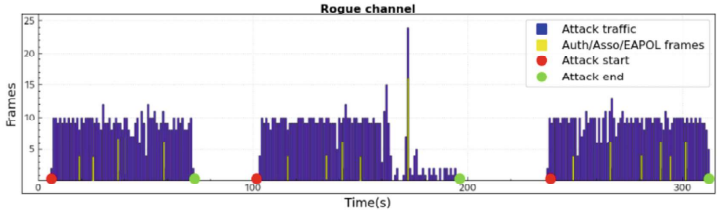


(b)

Fig. 11. Trace of network with beacon traffic on (a) operating channel; (b) rogue channel.



(a)



(b)

Fig. 12. Trace of network traffic having authentication and association frames and EAPOL messages on (a) operating channel; (b) rogue channel.

at most two authentication frames, two association frames, and four EAPOL frames on two distinct channels at a time. As a result, we adjust the thresholds for authentication, association, and EAPOL messages to 1 frame in order to quickly confirm this peculiar traffic in a probe interval duration when MC-MitM attacks happen.

Concurrent Data Traffic Signature. In Fig. 13, we show the network trace consisting of multiple data with two distinct channels using similar BSSID and SSID at the same time.

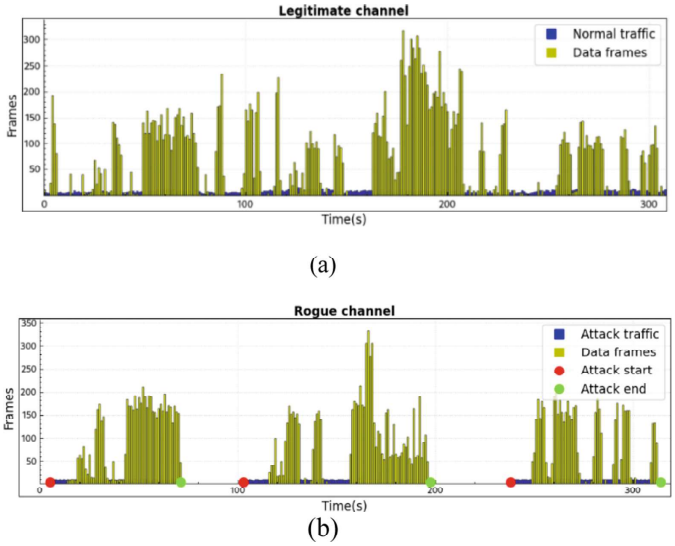


Fig. 13. Trace of network data traffic on (a) operating channel; (b) rogue channel.

As we can see Fig. 13, there can be large number of exchanged data frames on both operating and rogue channels. Further, we use this peculiar data traffic as an optional way to confirm MC-MitM attacks and adjust data traffic threshold to 1 frame in a probe interval duration.

4.5 Summary of Attack Traffic Signatures

In Table 4, we summarize distinct attack signatures that can be used to recognize deliberate MC-MitM attacks in a probe interval duration.

4.6 Discussion

As we demonstrated in the previous section, the designed attack signatures differ greatly from the normal Wi-Fi network behavior, which makes passive detection of MC-MitM attacks feasible. Furthermore, we set appropriate minimum threshold values so as to quickly detect different attacks. The proposed attack signatures are also lightweight

Table 4. Summary of MC-MitM attack signatures.

	Signatures of attack	Used metrics with threshold values
Stage 1 attack traffic	Constant jamming	FIAT $\geq$ 2 ms and FDR $<$ 50%
	Reactive Jamming	Malformed frame rate $\geq$ 50%
	Fake CSAs	Number of CSA $\geq$ 1
Stage 2 attack traffic	Concurrent beacon traffic	Number of beacons $\geq$ 1
	Concurrent connection traffic	Number of Auth/ Asso/EAPOL frames $\geq$ 1
	Concurrent data traffic	Number of data frames $\geq$ 1

and can be easily deployed in any Wi-Fi network, including IoT networks, without modifying any existing protocols. Furthermore, even though an attacker is aware of the deployed attack signatures, it is difficult for him to bypass. This is due to the fact that we defined the thresholds for identifying the appearance of malicious frames as part of the essential operations (i.e., stage 1 attack and stage 2 attack traffic) required for successful MC-MitM attempts, and it is impossible to carry out such attacks without meeting or surpassing those thresholds. Moreover, even if the attacker devises any other new tactics to deceive the victim besides jamming or CSA attacks as part of stage 1 attack, the stage 2 attack traffic signatures can predict the existence of such attacks.

5 Conclusions and Future Works

This paper provides researchers with an overview of MC-MitM attacks their ability to manipulate encrypted/protected wireless connections. We highlighted the security impacts of different MC-MitM attack exploits and various challenges to defending such attacks. To this end, we examined network behavior when MC-MitM attack happens. Afterwards, we designed lightweight signatures and selected appropriate metrics to quickly and passively distinguish MC-MitM attacks by conducting an empirical analysis about attack as well as normal behavior of the traffic. We showed that the attack signatures are quite different from normal Wi-Fi behavior. As a future work, we propose to implement a wireless intrusion detection system that utilizes different attack signatures created. Particularly, we aim to demonstrate and test it on a *Raspberry Pi* since it is widely used for establishing home automation domotic systems, such as Home Assistant and OpenHAB. Moreover, we plan to develop our system with a plug-and-play support, which facilitates easy integration into any wireless environments, including IoT networks without altering any existing devices or protocols.

Acknowledgements. This research work was funded by the Spanish Government through project PID2021-125962OB-C31 "SECURING".

References

1. Fajar, B.: Fluxion Kali Linux Tutorial. https://linuxhint.com/fluxion-kali-linux-tutorial/. Accessed 20 May 2021

2. KaliTut, WiFi Pumpkin Framework for Rogue WiFi Access Point Attack. https://kalitut.com/wifi-pumpkin-framework-for-rogue-wi-fi/. Accessed 25 May 2021
3. Vanhoef, M., Piessens, F.: Advanced Wi-Fi attacks using commodity hardware. In: Proceedings of the 30th ACM Annual Computer Security Applications Conference, pp. 256–265 (2014)
4. Vanhoef, M., Piessens, F.: Key reinstallation attacks: forcing nonce Reuse in WPA2. In: Proceedings of the ACM SIGSAC Conference on Computer and Communication Security, pp. 1313–1328 (2017)
5. Vanhoef, M.: Fragment and forge: breaking Wi-Fi through frame aggregation and fragmentation. In: 30th USENIX Security Symposium, pp. 161–178 (2021)
6. Thankappan, M., Rifà-Pous, H., Garrigues, C.: Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: a state of the art review. Expert Syst. Appl. **210**, 118401 (2022)
7. Freudenreich, J., Weidman, J., Grossklags, F.: Responding to KRACK: Wi-Fi security awareness in private households. In: Clarke, N., Furnell, S. (eds.) Human Aspects of Information Security and Assurance. HAISA 2020. IFIP Advances in Information and Communication Technology, vol. 593, pp. 233–243. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-57404-8_18
8. Philipp Ebbecke, Protected Management Frames enhance Wi-Fi network security. https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security. Accessed 20 May 2022
9. Gong,, S., Ochiai, H., Esaki, H.: Scan-based self anomaly detection: client-side mitigation of channel-based man-in-the-middle attacks against Wi-Fi. In: IEEE 44th Annual Computers, Software, and Applications Conference, pp. 1498–1503 (2020)
10. Vanhoef, M., Bhandaru, N., Derham, T., Ouzieli, I., Piessens, F.: Operating channel validation: preventing multi-channel man-in-the-middle attacks against protected wi-fi networks. In: Proceedings of the 11th ACM Conference Security and Privacy in Wireless and Mobile Networks, pp. 34–39 (2018)
11. Vanhoef, M., Adhikari, P., Pöpper, C.: Protecting wi-fi beacons from outsider forgeries. In: Proceedings of the 13th ACM Conference Security and Privacy in Wireless and Mobile Networks, pp. 155–160, (2020)
12. Van Goethem, T., Vanhoef, M., Piessens, F., Joosen, W.: Request and conquer: exposing cross-origin resource size. In: 25th USENIX Security Symposium, pp. 447–462 (2016)
13. Vanhoef, M., Piessens, F.: Predicting, decrypting, and abusing WPA2/802.11 group keys. In: 25th USENIX Security Symposium, pp. 673–688 (2016)
14. Vanhoef, M., Piessens, F.: Release the kraken: new kracks in the 802.11 standard. In: Proceedings of the ACM Conference on Computer and Communication Security, pp. 299–314 (2018)
15. Chi, M., Bu, B., Wang, H., et al.: Multi-channel man-in-the-middle attack against communication-based train control systems: Attack implementation and impact. In: Liu, B., Jia, L., Qin, Y., Liu, Z., Diao, L., An, M. (eds.) Proceedings of the 4th International Conference on Electrical and Information Technologies for Rail Transportation (EITRT) 2019. EITRT 2019. LNEE, vol. 640, pp. 129–139. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-2914-6_14
16. Louca, C., Peratikou, A., Stavrou, S.: On the detection of channel switch announcement attack in 802.11 networks. In: International Conference on Cyber Security, pp. 281–285 (2021)

17. Osanaiye, O., Alfa, A., Hancke, G.: A statistical approach to detect jamming attacks in wireless sensor networks. Sensors (Switzerland) **18**(6), 1691 (2018)
18. Woody, L.: mitm-channel-based-package. https://pypi.org/project/mitm-channel-based/. Accessed 10 June 2022
19. ETSI E: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive. Broadband Radio Access Networks. v1.8.1 (2012)

4

A Signature based Wireless Intrusion Detection System (SWIDS) Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-fi Networks

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 January 2024, accepted 27 January 2024, date of publication 6 February 2024, date of current version 16 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3362803

RESEARCH ARTICLE

A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks

MANESH THANKAPPAN[1,2], (Member, IEEE), HELENA RIFÀ-POUS[1,3], (Member, IEEE), AND CARLES GARRIGUES[1,3]

[1]Estudis d'Informàtica Multimèdia i Telecomunicació, Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), 08018 Barcelona, Spain
[2]Adi Shankara Institute of Engineering and Technology, Kalady, Ernakulam, Kerala 683574, India
[3]CYBERCAT-Center for Cybersecurity Research of Catalunya, 43003 Tarragona, Spain

Corresponding author: Manesh Thankappan (mthankappan@uoc.edu)

This work was supported in part by the Ministerio de Ciencia e Innovación, la Agencia Estatal de Investigación and the European Regional Development Fund (ERDF) under Project PID2021-125962OB-C31; and in part by the ARTEMISA International Chair of Cybersecurity and the DANGER Strategic Project of Cybersecurity, both funded by the Spanish National Institute of Cybersecurity through the European Union-NextGenerationEU and the Recovery, Transformation and Resilience Plan.

ABSTRACT One of the advanced Man-in-the-Middle (MitM) attacks is the Multi-Channel MitM (MC-MitM) attack, which is capable of manipulating encrypted wireless frames between clients and the Access Point (AP) in a Wireless LAN (WLAN). MC-MitM attacks are possible on any client no matter how the client authenticates with the AP. Key reinstallation attacks (KRACK) in 2017-18, and the latest FragAttacks in 2021 are frontline MC-MitM attacks that widely impacted millions of Wi-Fi systems, especially those with Internet of Things (IoT) devices. Although there are security patches against some attacks, they are not applicable to every Wi-Fi or IoT device. In addition, existing defense mechanisms to combat MC-MitM attacks are not feasible for two reasons: they either require severe firmware modifications on all the devices in a system, or they require the use of several advanced hardware and software for deployment. On top of that, high technical overhead is imposed on users in terms of network setup and maintenance. This paper presents the first plug-and-play system to detect MC-MitM attacks. Our solution is a lightweight, signature-based, and centralized online passive intrusion detection system that can be easily integrated into Wi-Fi-based IoT environments without modifying any network settings or existing devices. The evaluation results show that our proposed framework can detect MC-MitM attacks with a maximum detection time of 60 seconds and a minimum TPR (true positive rate) of 90% by short-distance detectors and 84% by long-distance detectors in real Wi-Fi or IoT environments.

INDEX TERMS Attack signature, FragAttacks, intrusion detection, Internet of Things (IoT), KRACK, multi-channel MitM (MC-MitM), Wi-Fi, WPA, WLAN.

I. INTRODUCTION

A. CONTEXT

WLANs are susceptible to a wide array of wireless security attacks. A Man-in-the-middle (MitM) attack is a critical security threat towards wireless networks in which the perpetrator is positioned in the middle of the communication between the client and the Access Point (AP), allowing the attacker to eavesdrop, manipulate messages, and impersonate one of the parties. In the simplest form of such attacks, the attacker introduces a laptop with two Wi-Fi cards; one of them is connected to the legitimate AP or his own AP, and the other acts as a

The associate editor coordinating the review of this manuscript and approving it for publication was Mostafa M. Fouda.

rogue AP (also known as an evil-twin), spoofing the target AP so that clients will connect to it because of the commonly used automatic AP selection option [1]. In general, there are two approaches to perform MitM attacks in a WLAN.

In the first approach, which we will refer to as a traditional rogue AP MitM attack from now on, the attacker launches a new rogue AP, forces the clients to connect to it using a known Wi-Fi passphrase, and then manipulates the encrypted traffic. Therefore, traditional rogue AP MitM attacks require a known Wi-Fi passphrase for manipulating encrypted traffic between the client and the AP. Fluxion [2], Wifiphisher [3], WiFi-Pumpkin [4], airbase-ng [5], etc. are some commonly employed traditional rogue AP MitM attack tools. The second approach, our research focus, is the Multi-Channel MitM (MC-MitM) attack, introduced by Vanhoef and Piessens in 2014 [6], which consists of two Wi-Fi cards operating on two different channels but maintaining a single connection to manipulate encrypted wireless traffic between the client and the legitimate AP on the fly without possessing any legitimate Wi-Fi passphrases.

The rationale behind the MC-MitM attack is to clone the legitimate AP on a different channel, which facilitates the attacker exchanging all connection establishment and data frames between both channels so that he can communicate with both the client and the AP simultaneously [6], [7]. Moreover, exchanging frames between different channels is possible no matter how the client authenticates with the network. Therefore, MC-MitM attacks can be used in personal as well as enterprise Wi-Fi networks. Once the MC-MitM position is acquired, the attacker can use other attacks to block and modify encrypted frames between the client and legitimate AP. We note that the MC-MitM position does not break any encryption but is primarily used to perform attacks to exploit specific weaknesses (e.g., flaws in authentication or encryption) in Wi-Fi standards such as WPA, WPA2, or WPA3. A comprehensive security analysis of different Wi-Fi standards is available in our previous paper [13]. Fundamentally, to acquire the MC-MitM position, the attacker either employs special jamming techniques or channel switch announcements (CSAs) to force the clients to switch to their channels. In this paper, we refer to jamming-based MC-MitM as base variant attacks and CSA-based MC-MitM as improved variant attacks.

The most well-known MC-MitM base variant attack is the key reinstallation attack (KRACK). KRACK exploits severe nonce reuse vulnerabilities (discovered by Vanhoef et al. in October 2017 [8]) during 4-way handshake mechanisms in the IEEE 802.11 standards. Such vulnerabilities enable the attacker to trivially decrypt Wi-Fi frames, especially from Linux and Android devices supporting WPA/2 standards. This was the first non-vendor-specific vulnerability that impacted millions of Wi-Fi devices due to a faulty implementation of the standard.

Regarding the MC-MitM improved variants, the most significant attacks include FragAttacks and some extended versions of KRACK attacks. The FragAttack is the latest non-vendor-specific attack using the MC-MitM position (discovered by Vanhoef in May 2021 [9]). It exploits a set of authentication weaknesses in the fragmentation and aggregation features of IEEE 802.11 standards allowing the attackers to inject packets into encrypted Wi-Fi networks and obtain sensitive client data.

The aforementioned MC-MitM attacks also affect WPA3 standards. Although patches are available for both KRACK and FragAttacks, the critical problem is that they are not applicable on every Wi-Fi or IoT device because of factors like resource constraints, deprecated security protocols, expired product support periods, etc. Four years after KRACK first appeared, it is estimated that more than 75 per cent of Wi-Fi enabled devices still remain vulnerable to it [10], [11].

MC-MitM attacks have been exploited in some critical systems. For example, [12] showed how the MC-MitM position could be applied to obfuscate train control systems to cause emergency braking and system collapse. Surprisingly, they used the MC-MitM position to capture, decrypt, and modify protected Wi-Fi packets (train control messages). In our previous paper [13], we evaluated the capabilities of MC-MitM attacks and provided a detailed description of the different kinds of MC-MitM attacks reported so far.

B. CHALLENGES IN DETECTING MC-MITM ATTACKS

Detecting MC-MitM attacks is challenging because the attacker spoofs almost every characteristic of the legitimate AP and the client (victim) simultaneously, and operates as legitimately as possible in the target Wi-Fi network. More specifically, the attacker does not conduct any flooding attack using spoofed beacons, probe requests, or other frames to deceive and acquire the clients. Therefore, the frame arrival rate-based detection technique is also not helpful. In MC-MitM attacks, the attacker collects the beacons of real AP and retransmits them on his rogue channel. As a result, MC-MitM attackers can evade snooping-based rogue AP detection techniques, such as [14] and [15] which are based on verifying whether RSSI values are higher than that of the legitimate AP. Moreover, the MC-MitM attacker can easily configure the transmission power and forge other features if he knows them [16]. Furthermore, researchers show the feasibility of using CSAs for launching MitM attacks even with relatively lower RSSI values than that of legitimate APs [17]. Therefore, relying on RSSI values alone may not be an effective defense.

Communication channels can also be monitored. However, checking beacons only on the legitimate channel is not always beneficial because there are valid reasons for an AP to switch to different channels. For example, channel switching is essential to avoid interference from radar noise on certain channels, and is a dynamic action in modern routers enabled by the Dynamic Frequency Selection (DFS) feature [18]. Furthermore, the MC-MitM attacker can use a special kind of constant jamming or reactive jamming by using cheap off-the-shelf Wi-Fi dongles in order to establish

the MitM position, which is relatively hard to detect by existing intrusion detection systems [6], [19]. This is because the MC-MitM attack transmits random noise pulses during jamming, which are interpreted as any non-Wi-Fi device using a similar frequency band.

Traditional perimeter security measures (e.g., firewall, VPN) are generally employed to protect sensitive communications in a WLAN. However, such measures cannot prevent MC-MitM attacks from directly attacking various Wi-Fi devices since such attacks are link-layer attacks, and firewalls deal with upper layers stack.

The Wi-Fi Alliance enforced Protected Management Frame (PMF) beginning in 2018, which provides integrity protection mechanisms for WPA2 and WPA3 protocols to prevent rogue AP MitM or DoS attacks [20], [21]. The use of PMF only achieves protection for certain robust management frames such as deauthentication, disassociation, and action frames [22]. However, PMF is not sufficient to defend against MC-MitM attacks. This is mainly because: 1) the attacker does not use deauthentication packets to acquire the MC-MitM position [23]; 2) PMF cannot detect jamming attacks [24]; and 3) MC-MitM attacks use beacons or probe responses, which PMF does not protect. Moreover, if the MC-MitM attacker is an insider (authorized user), he can even steer clients to switch to his rogue AP using CSA action frames [17], [25]. This makes such attacks difficult to detect in practice.

In the aforementioned scenarios, it is difficult to appropriately identify MC-MitM attacks. Although specific defense mechanisms have been proposed in the literature, they require modifications to the Wi-Fi protocol or advanced hardware or software to be deployed on each Wi-Fi client and/or AP and are therefore only effective if all devices on a WLAN are compatible with them. This stringent security requirement is not always achievable with IoT devices or every Wi-Fi client.

C. MOTIVATION

In our previous paper [13], we extensively studied the technical feasibility of various MC-MitM defense mechanisms and demonstrated that their deployment is difficult to achieve, especially in IoT environments such as smart homes. On the one hand, there are no patches for all commercial devices, and on the other hand, the management and maintenance of these devices requires technical knowledge that the average user does not have. Moreover, existing defense mechanisms cannot handle such attacks due to several interoperability issues. Hence, there is a need for effective defense mechanisms. Given these considerations, we have designed a lightweight and signature-based intrusion detection framework that is tailored to meet the demands of smart environments based on IoT. Rather than depending on machine learning, our detection framework scrutinizes wireless network frames to quickly recognize attack signatures or behaviors of malicious network activity. Our approach is a plug-and-play system that can be easily integrated into any Wi-Fi or IoT setup without requiring changes to network configurations or pre-existing devices, and it delivers consistent security against all types of MC-MitM attacks.

In real Wi-Fi or IoT environments, our short-distance detectors achieved a minimum True Positive Rate (TPR) of 90%, while our long-distance detectors achieved a TPR of 84%. Furthermore, we have evaluated our proposed framework using the AWID3 dataset [26], which is a publicly available dataset containing KRACK attack signatures. Our framework showed good performance (above 99% in accuracy) compared to other mechanisms that utilize the AWID3 dataset.

D. CONTRIBUTIONS

In this paper, we make the following contributions:

1) Classification and analysis of attack traffic in MC-MitM attacks.
2) Theoretical and empirical analysis of attack traffic and creation of potential attack signatures for MC-MitM attacks.
3) Design of the first plug-and-play signature-based wireless intrusion detection system framework that can be used in any Wi-Fi network.
4) Development of an open-source prototype [27] of the proposed framework using the python-scapy library.
5) Empirical evaluation of the proposed framework in an industry-relevant smart home environment with off-the-shelf IoT devices.

E. ORGANIZATION OF THE PAPER

The remainder of the paper is organized as follows: Section II briefly discusses the background and related work; Section III classifies the specific attack traffic during MC-MitM attacks and presents their behavior; Section IV presents an in-depth combination of theoretical and empirical analysis of attack traffic, creates attack signatures, and indicates metrics to identify MC-MitM attacks; Section V introduces our proposed solution and architectural units; Section VI presents an evaluation of the proposed solution. Finally, Section VII presents conclusions and future research work.

II. BACKGROUND AND RELATED WORK

We first outline the working principles of the MC-MitM attack and its variants. We then classify and describe existing defense mechanisms for MC-MitM attacks.

A. BACKGROUND

MC-MitM attacks can sniff and manipulate encrypted wireless communication (e.g., WPA, WPA2, or WPA3) between clients and the AP in a WLAN. In such attacks, the attacker's goal is to identify the channel of the legitimate AP and then clone it on a different channel to exchange frames between both channels. The said exchange of frames enables the attacker to legitimately communicate with both end devices (the client and legitimate AP) simultaneously. Once the

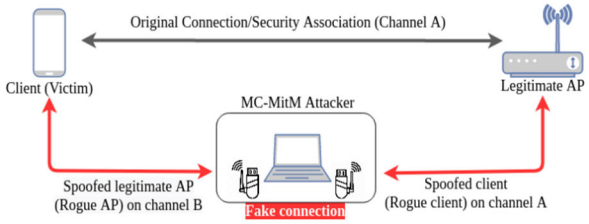


FIGURE 1. Multi-channel MitM Setup.

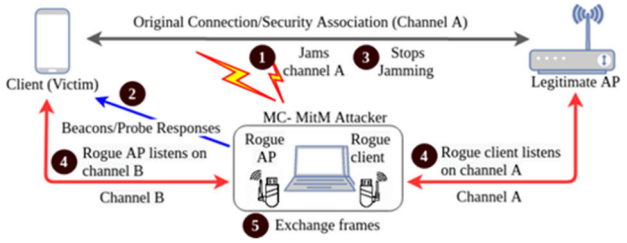


FIGURE 2. MC-MitM-BV attack.

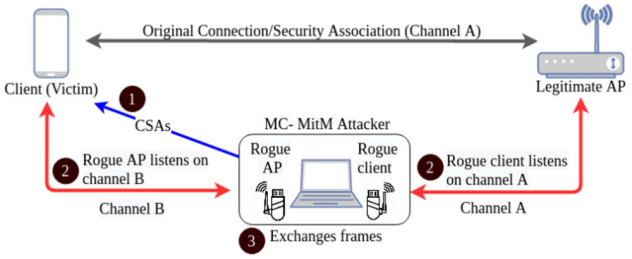


FIGURE 3. MC-MitM-IV attack.

MC-MitM position is acquired, the attacker can manipulate (e.g., delay, modify, inject, replay) encrypted frames between end devices. Figure 1 shows a typical MC-MitM attack setup. As we can see from Figure 1, the attacker uses two Wi-Fi dongles to spoof end devices on the opposite-side channel. Since both Wi-Fi dongles are physically close, they receive each other's frames even if they operate on two different channels.

The main advantage of employing the MC-MitM attack is that it does not require the legitimate Wi-Fi passphrase of a WLAN since the attacker does not break the original connection or security association between end devices. Thus, end devices retain a PMK (Pre-Master Key) stored in their Wi-Fi chips and use it for negotiating the same session key or PTK (Pairwise Transient Key) through a fake connection as shown in Figure 1. More specifically, the attacker exchanges authentication, association, and 4-way handshake frames between these two channels, which actually makes the end devices negotiate the same session key to encrypt the subsequent communication. This enables the MC-MitM attacker to bypass the authentication and 4-way handshake between the AP and the victim, capturing encrypted frames that can be manipulated by applying potential key reinstallation, aggregation, and fragmentation vulnerabilities.

In terms of forcing the clients towards the attacker, we classify MC-MitM attacks in two classes: base variant and improved variant.

1) BASE VARIANT

Vanhoef and Piessens introduced the MC-MitM base variant (MC-MitM-BV) attack in 2014 [6].

As shown in Figure 2, with this attack variant, the attacker: (1) jams the operating channel (channel A) of the legitimate AP (2) broadcasts beacons or probe responses (already collected from the legitimate channel A) instantly on the rogue channel (channel B) to force the client into connecting to his rogue AP (3) stops the jamming as soon as the client gets connected to the rogue AP (4) listens on channels B and A, respectively by the rogue AP and rogue client and (5) begins exchanging encrypted frames between the legitimate AP and client and vice versa.

Basically, two types of jamming techniques are used with this variant: constant jamming and reactive jamming. In this paper, we call MC-MitM-BV with constant jamming as MC-MitM-BVC and MC-MitM-BV with reactive jamming as MC-MitM-BVR attacks. When constant jamming is used, all the traffic on a target channel will be indiscriminately jammed while only specific frames (beacons or probe responses) are malformed with the reactive jamming. We highlight that jamming does not break the original security association. Instead, it just makes target networks unavailable for some time. As per the 802.11 standards, a client always chooses an available network or a network to which it was previously connected. Therefore, the victim switches with the available rogue AP by switching its channel and transmitting data on it. Some examples of MC-MitM enabled security downgrade attacks, KRACK, and DoS attacks performed using MC-MitM-BVC are described in the literature [6], [8], [28], [29], whereas in [19], MC-MitM-BVR is used.

2) IMPROVED VARIANT

Vanhoef and Piessens further proposed the MC-MitM improved variant (MC-MitM-IV) attack in 2018 [7], which is more practical compared to the MC-MitM-BV attack. As shown in Figure 3, with this attack variant, the attacker: (1) sends forged channel switch announcements (CSA) on channel B to force the clients into connecting to the rogue AP (2) listens on channels B and A, respectively by the rogue AP and rogue client and (3) begins exchanging encrypted frames between the legitimate AP and client and vice versa. The use of CSA significantly reduces the cost of jamming and the attacker's effort. Moreover, the attack requires only a few CSAs.

The use of CSAs is more reliable as it is an activity of the APs under radar noise conditions that the clients cannot decline. Similar to jamming, CSAs do not break the original security association. Instead, they instruct the client to switch to a new channel designated by the attacker. In addition, the attacker can transmit CSAs by forging a CSA information ele-

ment inside beacon frames, probe response frames, or action frames. Some prominent examples of MC-MitM-IV attacks, including KRACK, DoS, and the latest FragAttacks, have appeared in the literature [7], [9], [12], [30]. In Section III of our previous paper [13], we thoroughly explained the technical setup, inner workings, and extensive evaluation of various MC-MitM attacks that manipulate victim's data frames, resulting in frame decryption and potential extraction of sensitive data.

3) OTHER SPECIAL CAPABILITIES OF MC-MITM ATTACKS

The MC-MitM attacker behaves as normal in a WLAN and does not conduct any flooding attack using spoofed deauthentications, beacons, probe requests, or other frames to deceive and acquire the clients. Attackers can also circumvent IDS alerts with the special jamming methods employed in MC-MitM since they transmit noise pulses instead of injecting wireless frames [6]. Moreover, both attack variants can be effectively used against PMF-enabled devices. This is because management frames such as beacons or probe responses are not protected even if PMF is enabled. This ability enables the MC-MitM attacker to target the latest WPA2 and WPA3 devices as they use PMF by default [20]. Furthermore, the attacker can send CSA through action frames if he is an insider attacker, even when PMF is used [17]. It is also feasible to employ CSAs to acquire the MitM position from relatively longer distances with weaker signals [17]. Furthermore, the MC-MitM position facilitates the viability of certain MitM attacks such as chop-chop attacks [31], SSLStrip attacks [32], and Wi-Fi geolocation attacks [33], etc.

B. RELATED WORK ON DEFENSE MECHANISMS

We categorize the current defense mechanisms against MC-MitM attacks into two groups: stage 1 and stage 2 defense mechanisms. Stage 1 mechanisms aim to protect against attackers prior to obtaining the MC-MitM position by identifying genuine attack vectors, including rogue channels, rogue devices, or spoofed channel switch announcements. The second category concentrates on defending against MC-MitM enabled attacks (such as KRACK, cipher downgrades, and FragAttacks) after the attacker has gained control of the MC-MitM position.

1) STAGE 1 DEFENSE MECHANISMS

The authors of [34] introduced an Operating Channel Validation (OCV) technique to cryptographically validate the operating channel between two wireless stations. This technique proposes the utilization of a new Operating Channel Information (OCI) element as an extension to the 802.11 standards. During the 4-way handshake messages, the OCI element in EAPOL (Extensible Authentication Protocol over LAN) frames is authenticated to ensure that the sender and the receiver are using the same communication channels. Although the OCV has been ratified as a feature in IEEE standards, it is not compulsory in any of the WPA standards and has not yet been widely adopted in practical settings or implemented by device vendors. Furthermore, the OCV technique solely provides protection for PMF capable devices, as it requires the use of PMF to prevent unprotected channel switch announcements.

In another work, [16] proposed a beacon protection mechanism to defend against attacks that exploit unprotected beacons to prevent common rogue AP-based attacks and potential MitM attacks. They introduced an additional information element (IE) within each beacon, enabling clients to cryptographically verify the integrity of beacons when connecting to an AP. Similar to their previous defense mechanism [34], the beacon protection mechanism encounters practical challenges primary due to the requirement of PMF, which can create several interoperability issues while using devices supporting only WPA or WPA2 devices. Furthermore, the proposed mechanism does not block possible MC-MitM insider attacks, as demonstrated in [12].

In the WPA3-2020 updates, the WFA included another feature called Simultaneous Authentication of Equals-Public Key (SAE-PK) [35] to uniquely identify APs in a WLAN during the connection establishment process based on ECC (Elliptic Curve Cryptography) public key cryptography. SAE-PK also prevents insider attackers from setting up rogue AP and performing MitM attacks by using the using the AP's public key's digital signature. However, the detection of rogue APs is limited to the SAE-PK authentication phase or when the client initially connects to the AP. In contrast, an MC-MitM attacker typically positions themselves between an already connected client and the AP. The attacker can also bypass the SAE authentication because, according to [36], the WPA3 client uses an open authentication instead of an SAE authentication while reconnecting to an already connected network.

In [37], the authors proposed a defense mechanism based on Physically Unclonable Functions (PUF) to prevent rogue AP's actions during the MC-MitM attacks. Their approach involved generating a unique secret key from the AP's PUF signature and using it for mutual authentication between the AP and client devices. However, the PUF-based technique requires complex hardware modifications on all devices within a WLAN. Additionally, this method is vulnerable to certain types of MitM attacks [38].

In [19], the authors presented a defense method for Wi-Fi clients to detect rogue AP actions during MC-MitM-BVR attacks. They developed a patch for wpa_supplicant, an open-source implementation of Wi-Fi clients, to verify the uniqueness of a pair of identities such as SSID (Service Set Identifier) and BSSID (Basic Service Set Identifier) or when a client initiates a connection with an AP. However, the detection becomes challenging if the MC-MitM attacker employs continuous jamming on the legitimate AP channel, preventing the target client from retrieving and comparing the required beacon information. Moreover, relying solely on the uniqueness of the SSID and BSSID pair is not entirely

effective due to situations where the same pair of identities may be used. For example, if the AP supports a dual-band connection, there may be beacons with the same pair of identities.

2) STAGE 2 DEFENSE MECHANISMS

Most of the stage 2 defense mechanisms are intended to detect and mitigate MC-MitM enabled KRACK attacks due to their severe security impact on Wi-Fi systems. Various defense mechanisms such as [39], [40], [41], and [42] perform network analysis to identify a retransmitted or duplicated message 3 of the 4-way handshake mechanism during KRACK attacks. Nonetheless, as per the 802.11 standards, it is considered reasonable for an Access Point (AP) to retransmit message 3 in specific situations. This can occur when there is network traffic congestion or until the AP reaches its maximum retransmission limit. Consequently, indiscriminately blocking all retransmitted handshake message may lead to frequent handshake failures or increased false-positive rates.

In a recent study [43], an anomaly detection technique was proposed to identify handshake messages across multiple channels using supervised machine learning models, specifically targeting the detection of KRACK behavior. They used a state machine grouping algorithm to group retransmitted message 3 of the 4-way handshake on any channel other than the legitimate one. However, their focus was solely on detecting KRACK attacks. Similar works include [44], [45], and [46]. It is important to note that these machines learning based defense mechanisms have not been evaluated in real networks but rather assessed using the publicly available AWID3 dataset [26].

On the other hand, mechanisms described in [47], [48], and [49] propose new cryptographic verification techniques during the exchange of 4-way handshake messages to avoid nonce reuse weaknesses exploited by KRACK. These mechanisms also provide defense against cipher suite downgrade attacks on APs. However, the implementation of these proposals requires several changes to IEEE standards and has not been tested in real-world attack scenarios.

In [50], Snort rules are provided to detect network packets containing specific content (e.g., Dot11, RadioTap, FCfield) that may occur during the execution of KRACK attack tools or scripts. However, different implementations of the same KRACK attacks might not be detected by the current Snort rules. The content used by Snort rules to detect or match KRACK packets may even be present in legitimate WLAN packets or scripts of other tools and attacks developed using Scapy. Hence, relying solely on Snort with specific rules may prove ineffective or result in false alarms.

In order to protect against FragAttacks, there are currently no dedicated defense mechanisms available. However, there is a testing framework [51] for identifying fragmentation and aggregation vulnerabilities in Wi-Fi devices.

In general, the current defense mechanisms lack a comprehensive approach that can effectively detect all types of MC-MitM attacks. Additionally, a majority of these mechanisms have not undergone real-world evaluation in Wi-Fi or IoT environments, limiting their practical applicability. In Section VI-E, we present a comparison of the existing defense mechanisms, while in Section VI-F, we analyse the performance of systems that rely on the AWID3 dataset for evaluation purposes.

III. MULTI-CHANNEL MITM ATTACK ANALYSIS

In this section, we analyze the specific attack traffic related to different MC-MitM attack variants (see Section II-A). Towards this, we first classify MC-MitM attack traffic and then investigate the behavior of different attack variants.

Based on the behavior of MC-MitM attacks, we classify them into stage 1 attack traffic and stage 2 attack traffic. Stage 1 attack traffic appears first and indicates specific traffic during the acquisition of the MC-MitM position in Wi-Fi networks. Stage 1 attack traffic of MC-MitM-BVC and MC-MitM-BVR, respectively, can be the behavior of the network due to constant jamming and reactive jamming attacks; in the case of MC-MitM-IV, stage 1 traffic is the fake CSAs. Soon after the stage 1 attack traffic, i.e., after acquiring the MC-MitM position, stage 2 attack traffic arrives, which shows the behavior of the network when the attacker establishes two fake connections and exchanges authentication, association, 4-way handshake frames, and data frames between the client and the legitimate AP. Both MC-MitM attack variants exhibit similar stage 2 attack traffic.

A. ANALYSIS OF STAGE 1 ATTACK TRAFFIC

This section describes the specific network behavior of stage 1 attack traffic in terms of constant jamming, reactive jamming, and CSA attacks.

1) CONSTANT JAMMING ATTACK

When the attacker initiates a constant jamming attack targeting the operating channel of the AP, all traffic on that channel will be jammed indiscriminately. This means that there will be no Wi-Fi frames on a particular channel until the constant jamming stops. In particular, the MC-MitM attacker usually employs a specific type of constant jamming by transmitting noise pulses for a specific period of time. For instance, the attacker uses a jammer firmware with its Carrier Sense Multiple Access (CSMA) mechanism disabled, so that it injects random energy pulses to make the target channel appear to be always busy. As a result, nearby transmitters (APs) operating on the targeted channels would not send Wi-Fi frames, or clients would remain idle until the jamming on the AP's channel ends. This helps the MC-MitM attacker to force the clients to connect to the same or a cloned network, but on a different channel. The main advantage of this type of constant jamming attack is that it cannot be detected by intrusion detection systems. This is because instead of injecting random Wi-Fi frames, the tool transmits random noise pulses that would be seen as coming from any non-Wi-Fi device using a similar frequency band [6].

2) REACTIVE JAMMING ATTACK

The reactive jamming attack aims to jam beacons and probe responses from a target or AP's channel. The attacker first identifies the frames based on the MAC address and decodes the header on the fly while blocking the reception of the frames by the clients or victims. This is achieved by injecting dummy frames transmitted at higher data rates that resemble the original frames. This injection of dummy frames induces a collision and interference with the targeted beacons or probe responses. Subsequently, the FCS (Frame Check Sequence) of the targeted frame becomes incorrect or malformed, causing clients to ignore it or lose their connection to the AP. As a result, clients choose to connect to the cloned network of the MC-MitM attacker operating on a different channel. Like the constant jamming attack, the reactive jamming attack is also relatively difficult for intrusion detection systems to detect [19].

3) CHANNEL SWITCH ANNOUNCEMENT ATTACK

According to the IEEE standards [52], the channel switch announcement (CSA) is a normal behavior of an AP operating in the 5 GHz frequency bands with dynamic frequency selection (DFS) feature enabled. Typically, CSAs arrive with beacons or probe responses when the AP changes its channel due to the reception of radar pulses after booting up. The DFS feature allows the AP to use specific 5 GHz channels reserved for certain high-priority radar signals used for airport, military, satellite communications and meteorological purposes [18], [33], [53]. When the AP detects any of the high-priority radar signals mentioned above, it sends a CSA to all of its associated clients in order to switch to another 5 GHz channel. Further regulatory specifications for channel selection and DFS features can be found in [53].

CSAs can be easily spoofed regardless of the 2.4 or 5 GHz frequency band, due to the lack of appropriate authentication mechanisms for beacons and probe responses [34]. In either case, all Wi-Fi clients honor such CSAs by immediately switching channels. This allows the MC-MitM attacker to force channel switching using fake CSAs. To send fake CSAs, MC-MitM attackers first collect beacons and probe response frames from the legitimate AP and modify the spoofed CSA information element in them before transmitting them towards the targeted clients. With CSAs, the AP does not immediately switch to a new channel. Instead, it sends a certain number of beacons (the default is 4 CSA beacons as per the IEEE 802.11h standard) containing the CSA before switching to the new channel [53]. However, CSAs under the following three scenarios can be considered fake CSAs.

Scenario 1: The CSAs present in 2.4 GHz Wi-Fi networks must be considered fake CSAs as DFS does not apply to such Wi-Fi networks. This is critical because many home networks operate in the 2.4 GHz band, especially IoT devices.

Scenario 2: In 5 GHz Wi-Fi networks with DFS disabled, no CSAs can occur and those that do should be considered fake.

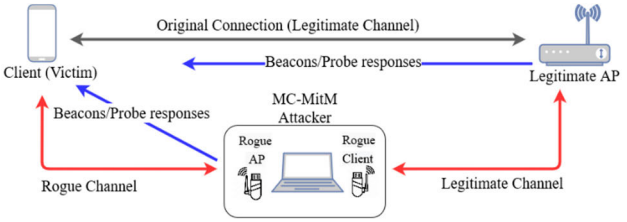


FIGURE 4. Concurrent beacon and probe response traffic.

Scenario 3: When the AP operates in the 5 GHz band and is booted (enabled) with the DFS feature, it first scans for radar signals as part of the Channel Availability Check (CAC) mechanism. Additionally, the AP continuously monitors the operating channel for radar signals throughout its lifetime and only switches to available DFS channels if such signals are detected [53]. DFS can be useful in home networks merely to find the best 5 GHz channel while powering up the AP. On the other hand, DFS is usually advisable for outdoor Wi-Fi devices or networks near airports, weather stations or military radars. Although this scenario is genuine for CSA occurrence when radar signals are detected, such signals are unusual events in home networks. Hence, the occurrence of such CSAs can be considered a warning sign of fake CSAs.

B. ANALYSIS OF STAGE 1 ATTACK TRAFFIC

This section describes the different network behaviors of stage 2 attack traffic.

1) CONCURRENT BEACON AND PROBE RESPONSE TRAFFIC

Concurrent beacon or probe response traffic corresponds to specific traffic that occurs simultaneously on two different channels (belonging to the same frequency band, 2.4 or 5 GHz) with the same SSID and BSSID and other parameters. Figure 4 shows the scenario of concurrent beacon or probe response traffic (blue colored arrows) arrival in a WLAN.

In WLANs, each AP transmits beacons periodically with an interval of 102.4ms. Beacons are essential to announce the presence of a network that synchronizes connected clients. Accordingly, soon after the stage 1 attack, the MC-MitM attacker copies the beacons from the operating channel of the legitimate AP and retransmits them on the rogue channel using his rogue AP. On the other hand, the legitimate AP continues transmitting beacons on its operating channel. This scenario results in the presence of concurrent beacon frames on two different channels immediately after the stage 1 attack.

Similarly, when a Wi-Fi client comes into proximity with previously connected networks in the Preferred Network List[1] (PNL), it starts scanning by sending probe requests to check for available Wi-Fi networks. The PNL, residing in the device's Wi-Fi chip, holds SSIDs and necessary connection details. In response, APs within the network send unicast

[1]PNL is stored in the device's Wi-Fi chip. It is a data structure with the list of SSIDs and any necessary credentials (passwords) for connecting.

probe responses, addressing the client's MAC, and relay information like SSID, BSSID on its operating channel. In the event of jamming or channel switching, clients in a particular network lose connection with the legitimate AP. As a result, the client broadcasts probe requests towards the visible rogue AP, resulting in the arrival of probe response frames to the clients on the rogue channel. On the other hand, the legitimate AP continues to send genuine probe responses to its clients on its operating channel. This scenario results in the presence of concurrent probe response frames on two different channels with the same SSID and BSSID during MC-MitM attacks.

However, such concurrent traffic is infeasible in Wi-Fi networks. The reason is that wireless networks operate on a single channel throughout their uptime or use a single channel to communicate with clients. Thus, the occurrence of such concurrent traffic can be considered an attack.

2) CONCURRENT CONNECTION ESTABLISHMENT TRAFFIC

In addition to concurrent beacon or probe response traffic, during MC-MitM attacks there will be concurrent connection establishment traffic such as authentication, association, EAPOL message exchanges on two different channels with the same SSID and BSSID. Such concurrent connection establishment traffic is essential to maintain the security association between the client and the legitimate AP, allowing them to negotiate the same session key through the MC-MitM setup (see Section II-A). Figure 5 illustrates the scenario of different types of concurrent connection establishment traffic.

When a Wi-Fi client receives probe responses from a previously connected AP, it establishes a connection with that AP on the designated channel. In the case of MC-MitM attacks, the client connects to the rogue AP (with the same SSID and BSSID of the legitimate AP) by sending an 802.1x open authentication frame on the rogue channel. At this moment, as shown in Figure 5(a), the MC-MitM attacker does the following: (1) captures the authentication request from the rogue channel using the rogue AP, (2) retransmits the captured authentication request on the legitimate channel using the rogue client, (3) captures the subsequent authentication response from the legitimate AP using the rogue client, and (4) retransmits the captured authentication response back to the rogue channel using the rogue AP. These frame exchanges constitute concurrent authentication traffic on two different channels with the same SSID and BSSID in a WLAN.

Similarly, the MC-MitM attacker exchanges association frames between two different channels, resulting in concurrent association traffic (see Figure 5(b)). Following the association traffic, the legitimate AP starts a 4-way handshake connection, consisting of four EAPOL messages. Consequently, the MC-MitM attacker collects each of such EAPOL frames from its originating channel and retransmits them on the other channel. Figure 5(c) shows the concurrent EAPOL traffic.

All combined, the above-discussed frame exchanges induce concurrent connection establishment traffic on two different channels with the same SSID and BSSID during MC-MitM attacks. On the other hand, such traffic is unfeasible in Wi-Fi networks because each Wi-Fi client tries to connect to the AP through a single channel at the same time.

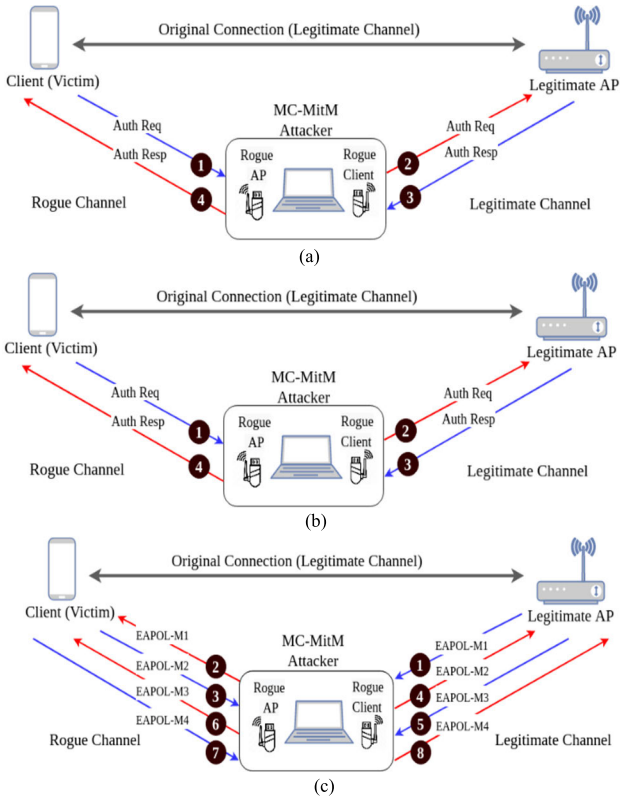


FIGURE 5. Concurrent connection establishment with (a) authentication traffic; (b) association traffic; (c) EAPOL traffic. Blue arrows indicate capturing frames and red arrows indicate retransmitting frames. Numbers on arrows indicate the order of exchange.

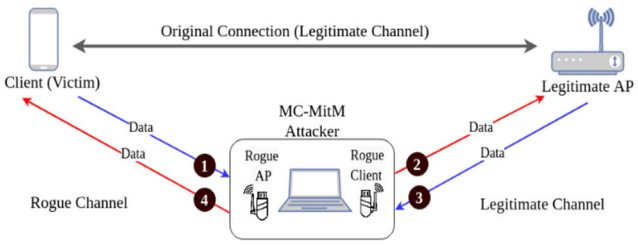


FIGURE 6. Concurrent data traffic. Blue arrows indicate capturing frames and red arrows indicate retransmitting frames. Numbers on arrows indicate the order of exchange.

3) CONCURRENT DATA TRAFFIC

Soon after the connection establishment traffic, both the client and the legitimate AP start communicating by encrypting their data. At this point, as explained in Figure 5, the MC-MitM attacker collects each data frame from its originating channel and retransmits it on the other channel (see Figure 6) to facilitate the communication between the client and the legitimate AP. This results in concurrent data traffic on two different channels with the same SSID and BSSID.

Yet, concurrent data traffic is unfeasible in Wi-Fi networks because the AP only transmits data on its operating channel to communicate with clients in a WLAN.

IV. SIGNATURE CREATION FOR MC-MITM ATTACKS

In this section, we present the stage 1 and stage 2 attack traffic signatures of MC-MitM attacks that we have determined from the network traffic behaviour presented in the previous section. These signatures are based on thresholds that can trigger the detection of these MC-MitM attacks. As we will see, some thresholds are derived from the theoretical analysis of the Wi-Fi protocol, while others are determined using an empirical analysis. We have employed a threshold-based approach in order to passively detect these MC-MitM attacks, since this is cost-effective and faster compared to machine learning-based solutions. Such signatures and their thresholds are used later in Section V, where we present the complete framework for the detection of MC-MitM attacks.

A. REFERENCE SCENARIO AND DETAILS OF EMPIRICAL ANALYSIS

We set up our reference scenario (see Figure 7) in our university research lab. It consists of three Wi-Fi clients (a smartphone and a laptop as WPA2 clients and another laptop as a WPA3 client) and an AP that operates in transition mode to provide WPA2 and WPA3 networks. We implement MC-MitM-BVC and MC-MitM-BVR attacks using the ModWifi platform [54] and MC-MitM-IV attacks using the multi-channel MitM package [55]. We also deploy different MC-MitM attacks interchangeably on WPA2 and WPA3 clients. We acquire the MC-MitM position and capture the traffic between the clients and the AP using Wireshark software.

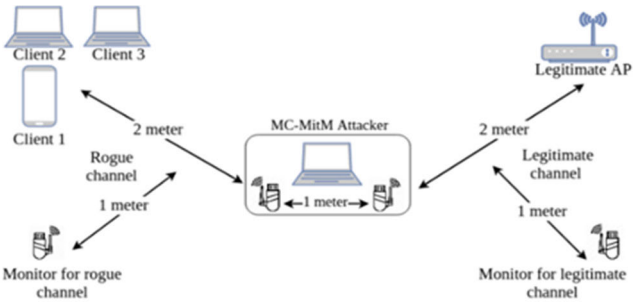


FIGURE 7. Reference attack scenario.

We also capture and thoroughly analyze the benign wireless traffic in different WPA2 or WPA3 based wireless networks, including enterprise (university) networks, home networks, and public networks to study their behavior. In the following sections, we monitor the traffic generated by abovementioned attacks over a specific period of time. From now on, we will refer to this period as the probe interval.

B. DESIGNING SIGNATURES OF STAGE 1 ATTACK TRAFFIC

In this section, we design signatures of the stage 1 attack traffic. Such signatures will be used as warning signs of imminent MC-MitM attacks. To do so, we monitor various types of stage 1 attack traffic (see Section III-A) specifically on the legitimate channel (operating channel) of the AP. This is because MC-MitM attackers first aim to interrupt connection between a victim and an AP on its designated operating channel.

TABLE 1. The resulting FIAT and FDR of Beacons in attack and benign traffic.

	FIAT (ms)		FDR (%)	
	AVG	SD	AVG	SD
Attack traffic	5	1.5	30	5.7
Benign traffic	0.1	0.02	90	1

1) CONSTANT JAMMING ATTACK

A constant jamming attack continuously produces high power noise that represents random bits on the AP' channel. Such attacks also act as intermittent jamming when the attacker stops and restarts MC-MitM attacks, causing sudden drops in frame availability. A drop in the wireless data reception can be detected using packet inter-arrival time (PIAT) and packet delivery ratio (PDR) metrics [56], [57]. In this paper, we refer to the above metrics as frame inter-arrival time (FIAT) and frame delivery ratio (FDR), as we analyze the MAC layer behavior of constant jamming attacks. Further, FIAT can be defined as the time elapsed between the reception of a frame and the next frame, whereas FDR is the ratio of the number of successfully delivered frames to the number of frames transmitted by the AP.

We have taken into account both of these metrics, since they can collectively signify intentional constant jamming activity. In our experiment to study constant jamming attacks, we calculate FIAT and FDR using beacon frames. Theoretically or as per standards [58], a Wi-Fi router typically transmits beacons every 100 milliseconds, resulting in the transmission of 10 beacons per second. In addition, it's crucial that the client successfully receives these beacons with a FIAT of 0.01 milliseconds so as to retain the Wi-Fi connection. Hence, we consider the above values as the foundation for establishing FIAT and FDR thresholds. We prepare the experiment by setting up a wireless connection between a client and an AP. Then, we start a probe interval of 60 seconds in which we first switch on the constant jamming for 30 seconds and monitor the network for 30 more seconds. We repeat the experiment 50 times. For each probe interval, we calculate the FIAT and FDR, and compare their values (average and standard deviation) with benign traffic (no attacks). Table 1 shows the resulting average (AVG) and standard deviation (SD) of FIAT and FDR in attack and benign traffic scenarios from our experiments.

As shown in Table 1, there is a significant variation in the FIAT and FDR values during intentional constant jamming

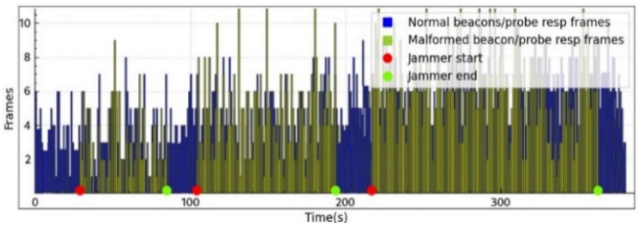


FIGURE 8. Attack traffic during a reactive jamming attack.

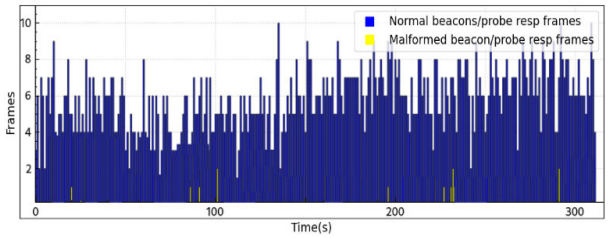


FIGURE 9. Benign traffic with malformed beacon/probe response frames.

attacks compared to the benign traffic. Accordingly, we set a FIAT threshold (TH1) of 2 ms and an FDR threshold (TH2) of 50% to identify the behavior of constant jamming attacks and provide a warning sign of possible MC-MitM-BVC attacks.

2) REACTIVE JAMMING ATTACK

We monitor the behavior of an intentional reactive jamming attacks during a 5-minute probe interval. During this time, we mount 3 periods of reactive jamming for 60, 100, and 150 seconds, as shown in Figure 8. We then separately capture frames during each period and found that more than 90% of the targeted beacons or probe response frames were malformed due to incorrect FCS.

On the other hand, the chances of occurrence of malformed frames in a Wi-Fi network can vary depending on various factors. These factors may include network conditions, the quality of hardware and software, interference, frame aggregation, and the presence of malicious actors. Theoretically, malformed frames should be non-existent and, in a well-maintained and secure network, the chances of malformed frames should be minimal [58].

As shown in Figure 9, when we analyse the benign traffic from the same AP for a probe interval of 15 minutes, we found only a negligible amount (less than 0.8%) of malformed beacon or probe response frames (with incorrect FCS). Such malformed frames are mainly due to incorrect frame reassembly or wrong frame size, which are common phenomena in wireless networks.

On the contrary, specific traffic consisting of malformed beacons or probe responses at higher rates (above 50%), especially on the operating channel of the AP, can be a good attack signature to indicate an intentional reactive jamming attack. Accordingly, we set the malformed rate threshold (TH3) to 50% in order to detect behavior of reactive jamming

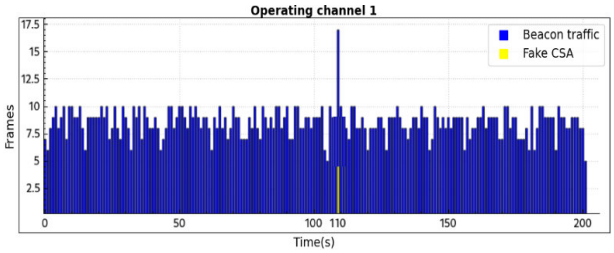


FIGURE 10. Traffic during fake CSA attack.

attacks during a probe interval and provide a warning sign for possible MC-MitM-BVR attacks.

3) CHANNEL SWITCH ANNOUNCEMENT ATTACK

CSA attacks can be conducted in three scenarios as discussed in Section III-A.3. The first two scenarios clearly identify an attack. To verify the third scenario (when an AP operates on 5 GHz with DFS enabled), we monitor the DFS characteristics in our home network for six months and confirm that the operating channel has not been changed. This supports our assumption that radar signals are uncommon in home networks. Therefore, the occurrence of CSAs can be considered as dubious network traffic even when DFS is enabled.

Figure 10 provides a view of fake CSA attacks on the AP's operating channel. It shows the traffic generated by the beacons on the operating channel of the AP even after the occurrence of CSAs at around 110 seconds, which should not happen when a genuine CSA occurs. This happens because the legitimate AP is unaware of the spoofed CSAs sent by the attacker, and it keeps broadcasting beacons on the same channel.

To study the behavior of benign traffic in home networks when a genuine CSA occurs, we invoked a channel switch (from channel 36 to 40) on a hostapd (access point daemon software) by sending the CSA command over the hostapd_cli interface [59].

Figure 11 depicts the behavior of traffic during a genuine channel switch. Here, we monitored the operating channel 36 and the new channel 40 simultaneously and observed that there is no traffic on operating channel 36 (see Figure 11(a)) after the occurrence of CSAs at around 100 seconds. At the same time, the legitimate AP begins its traffic on the new channel 40 only after 100 seconds (see Figure 11(b)).

In addition, we collected some real CSAs from a location near an airport by wardriving or sniffing on different DFS channels. For example, we observed a CSA instructing to switch from channel 60 to channel 64. We then monitored both channels simultaneously using the BSSID of the AP for a period of time (60 to 180 seconds) and were only able to collect traffic on the new channel 64, which is the same behavior as explained in Figure 11.

In essence, when a channel switch occurs, the AP stops transmitting on the current channel and starts transmitting on the newly designated channel. In accordance with

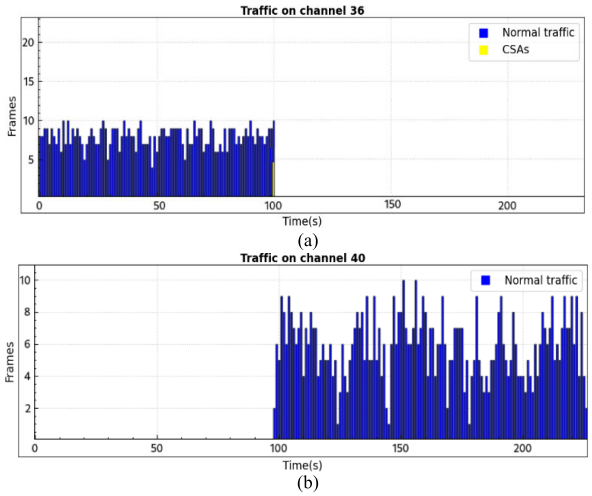


FIGURE 11. Traffic during a genuine channel switch on (a) current channel; (b) new channel.

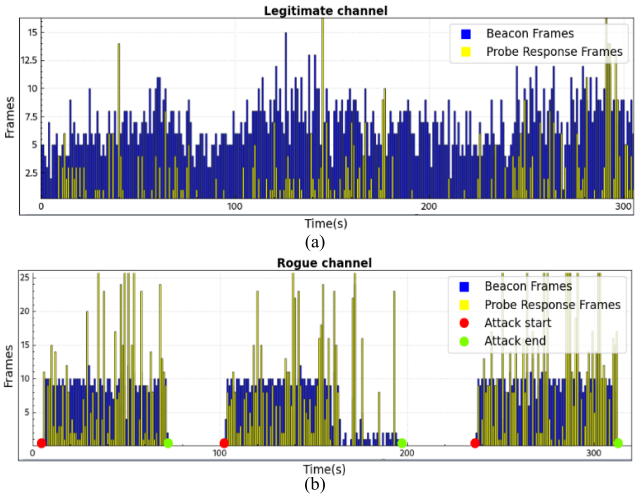


FIGURE 12. Attack network trace with beacons and probe responses on (a) legitimate channel; (b) rogue channel.

standards [58], a Wi-Fi network may typically experience 4 or 5 CSA frames during a channel switch. This can be observed in both Figure 10 and Figure 11, which respectively depict the CSA scenarios for attack and benign traffic. These observations serve as the foundation for establishing the threshold (TH4) to 1 CSA frame. Thus, we can quickly identify potential fake CSA frames and provide a warning sign for possible MC-MitM-IV attacks.

DFS detectors can also be used to verify the occurrence of CSAs [18]. However, such detectors recognize radar pulses and require advanced device setup, increasing the cost of attack detection significantly. This is the reason why, instead, we propose a simple way to detect potentially fake CSAs, and then we employ the attack signatures discussed in the following section to finally confirm the detection of an attack.

C. DESIGNING SIGNATURES OF STAGE 2 ATTACK TRAFFIC

In this section, we design signatures of stage 2 attack traffic (see Section III-B) to distinguish and confirm the presence of MC-MitM attacks. Furthermore, to identify the stage 2 attack traffic, we simultaneously monitor the legitimate APs and the rogue channels used for a probe interval of 5 minutes. We then launch 3 periods of MC-MitM attacks for 60-100 seconds.

1) CONCURRENT BEACON AND PROBE RESPONSE TRAFFIC

Figure. 12 shows an attack network trace with concurrent beacons and probe responses on two different channels with the same SSID and BSSID. We also analyze benign traffic scenarios, and we have not been able to detect any concurrent beacon or probe response traffic on multiple channels in the same frequency band with the same SSID and BSSID in the target Wi-Fi network.

On the other hand, there may be concurrent beacons if home APs broadcast the same SSID when operating on dual-band frequencies (both 2.4 GHz and 5 GHz). However, such concurrent beacons can be easily distinguished as benign traffic since the channels used in the 2.4 and 5 GHz bands are different.

Therefore, the sudden arrival of a significant number of concurrent beacons or probe response traffic on two different channels with the same SSID and BSSID in a WLAN, following the warnings generated by the stage 1 traffic analysis (see Section IV-B), clearly indicate the beginning of MC-MitM attacks. Accordingly, we set the threshold (TH5) to 1 beacon or probe response frame for quicker identification of concurrent beacon or probe response traffic accompanying the MC-MitM attacks during a probe interval. Furthermore, we confirm the presence of MC-MitM attacks by using the subsequent concurrent traffic in a WLAN.

2) CONCURRENT CONNECTION ESTABLISHMENT TRAFFIC

In Figure 13, we show an attack network trace with concurrent authentication frames on two different channels with the same SSID and BSSID. Figure 14 shows an attack network trace with the presence of concurrent association request and response frames on two different channels with the same SSID and BSSID. Finally, Figure 15 shows an attack network trace with the presence of concurrent EAPOL frames on two different channels with the same SSID and BSSID. The traffic shown in these three figures is only possible when an attack is in process, as no such concurrent traffic can occur on different channels with the same SSID/BSSID.

Therefore, this concurrent connection establishment traffic can be used as an attack signature to detect the presence of MC-MitM attacks in a WLAN. Taking this into account, we set the threshold (TH6) to 1 authentication, association, and EAPOL frames accompanying the MC-MitM attacks during a probe interval. This enables a fast identification of concurrent traffic.

3) CONCURRENT DATA TRAFFIC

Figure 16 shows an attack network trace with concurrent data on two different channels with the same SSID and BSSID.

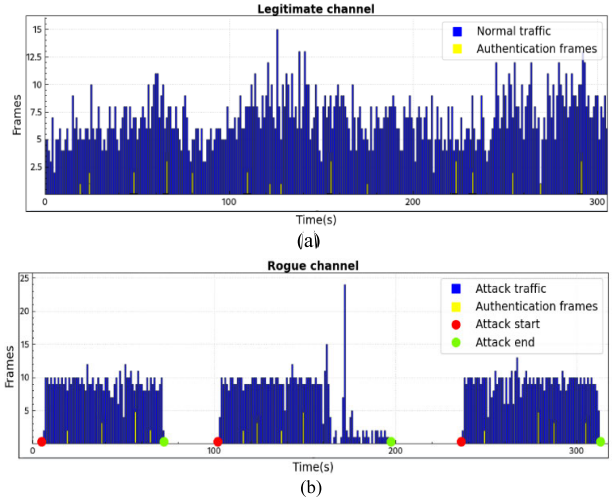


FIGURE 13. Attack network trace with concurrent authentication frames on (a) legitimate channel; (b) rogue channel.

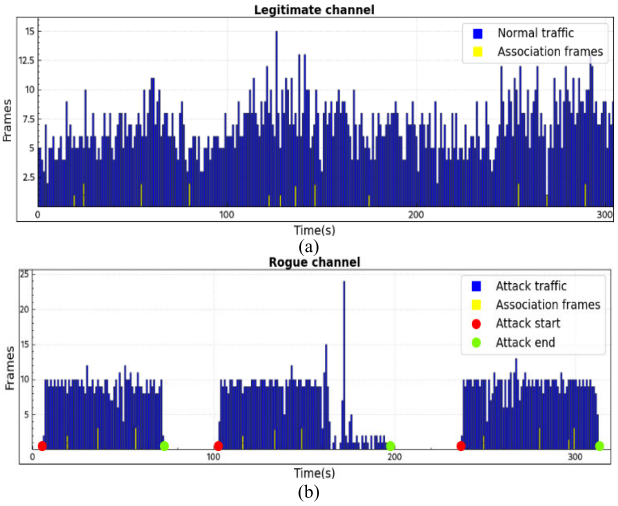


FIGURE 14. Attack network trace with concurrent association frames on (a) legitimate channel; (b) rogue channel.

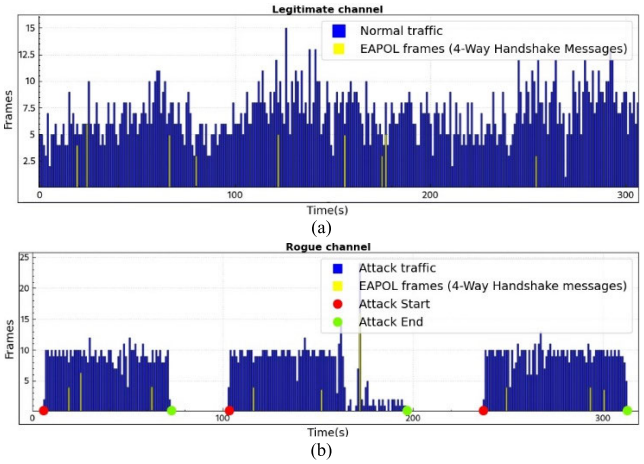


FIGURE 15. Attack network trace with concurrent EAPOL frames (4-Way Handshake messages on (a) legitimate channel; (b) rogue channel.

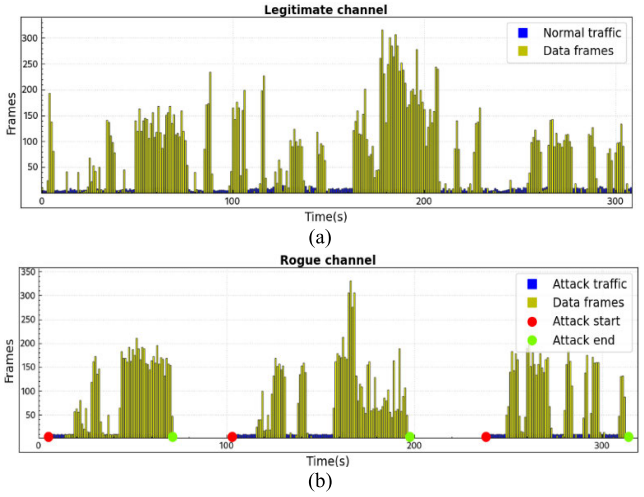


FIGURE 16. Attack network trace with data frames on (a) legitimate channel; (b) rogue channel.

As in the previous case, the data frames exchanged between the legitimate and rogue channels with the same SSID/BSSID can be used as a trigger for attack detection, since they are impossible considering the Wi-Fi protocol's normal operation. Therefore, we set the threshold (TH7) to 1 data frame for quicker identification of concurrent data traffic.

D. SUMMARY

Table 2 summarizes the attack signatures we propose for the detection of MC-MitM attacks during a probe interval. We must emphasize that thresholds TH4, TH5, TH6 and TH7 are grounded on the theoretical analysis of the operation of the Wi-Fi protocol. This makes it impossible for the MC-MitM attacker to execute an attack and remain undetected, unless some frames are missed due to network failures.

The remaining thresholds (TH1, TH2, TH3), instead, are derived from our empirical analysis and, therefore, we must admit that we cannot claim with complete certainty that no attack will go undetected in stage 1 using those thresholds. However, our empirical analysis and validation results shown in Section VI show that those thresholds are still very useful and can detect attacks in stage 1.

Even in the case that an attack was undetected in stage 1, we must emphasize that our protocol has two stages, and we can ensure that our approach would detect this attack in stage 2, because stage 2 uses only theoretical thresholds that no attack can elude (unless network conditions result in significant frame loss and this affects the detector's capabilities).

We also remark that, although stage 2 attack traffic can be used to detect MC-MitM attacks, both stage 1 and 2 attack signatures are necessary to distinguish between the MC-MitM different attack variants.

TABLE 2. Summary of attack signatures.

	Attack signature	Metrics used	Thresholds
Stage 1 attack traffic	Constant jamming	FIAT and FDR	TH1 ≥ 2 ms for FIAT and TH 2 < 50% for FDR
	Reactive Jamming	Malformed frame rate	TH3 ≥ 50%
	Fake CSAs	Number of CSAs	TH4 ≥ 1
Stage 2 attack traffic	Concurrent beacon traffic	Number of beacons or probe responses	TH5 ≥ 1
	Concurrent connection establishment traffic	Number of authentications, associations, or EAPOL frames	TH6 ≥ 1
	Concurrent data traffic	Number of data frames (optional metric)	TH7 ≥ 1

Furthermore, the datasets created in this work (attack network traces captured in the form of PCAP format with MAC layer frames) are made available in [60]. Our dataset is the first of its kind to provide traffic specifically from MC-MitM attacks and their variants.

V. PROPOSED SOLUTION: A SIGNATURE-BASED WIRELESS INTRUSION DETECTION FRAMEWORK FOR MC-MITM ATTACKS

In this section, we present the system architecture of the proposed solution, its architectural units, and the methodology to detect MC-MitM attacks by using attack signatures (malicious frames) discussed in the previous section.

A. SYSTEM ARCHITECTURE

Our proposed framework is based on a plug-and play, centralized, online passive monitoring system that can be easily integrated into any Wi-Fi or Wi-Fi-based IoT network. As presented in the previous section, we perform a signature-based network analysis to quickly and accurately detect abrupt and highly deviating changes in the network traffic due to MC-MitM attacks. Our framework is independent of the encryption techniques (WPA, WPA2, or WPA3), personal or enterprise networks, PMF standards, and Wi-Fi frequency bands (2.4 and 5 GHz) used in Wi-Fi networks.

Figure 17 shows the high-level system architecture of our proposed framework with overall workflow. It composed of four main units: traffic interceptor, device database unit, MC-MitM detection coordinator unit, and alert generator unit.

Below, we provide brief description of various units:

1) TRAFFIC INTERCEPTOR UNIT

The traffic interceptor unit passively monitors network traffic in a WLAN and collects suitable management frames (beacons, probe responses, action frames, connection establishment frames). This unit filters required frames based on

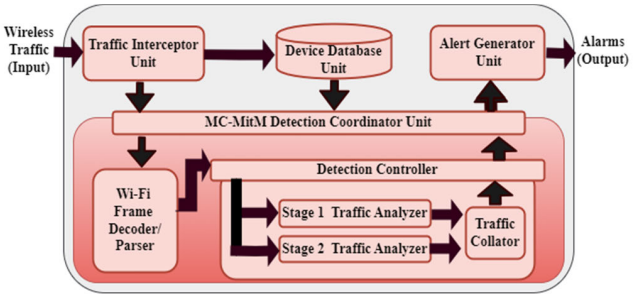


FIGURE 17. High-level system architecture.

MAC address of the AP and forwards them to the device database unit and the MC-MitM detection coordinator unit for further analysis.

2) DEVICE DATABASE UNIT

This unit automatically collects MAC addresses of clients connected to the legitimate AP in the targeted WLAN. Such information is provided to the MC-MitM detection coordinator unit to facilitate network analysis and scrutiny.

3) MC-MITM DETECTION COORDINATOR UNIT

This unit acts as the center of the detection process. Its main job is to analyze the network traffic and coordinate various processes to identify attack signatures associated with MC-MitM attacks during a probe interval. This unit also hosts the following two modules.

- **Wi-Fi frame decoder:** This module filters and analyzes network traffic between the AP and legitimate clients in a WLAN. It extracts low-level MAC layer header details from each frame, including type, subtype, ESSID, BSSID, operating channel, and more. These parsed frames are then sent to the detection controller.
- **Detection controller:** This module implements a detection methodology (see Section V-B) to identify the specific traffic associated with MC-MitM attack variants. It has three sub-modules. Sub-modules, such as stage 1 and stage 2 traffic analyzers, respectively, record the number of network frames that correspond to the stage 1 and stage 2 attack signatures (see Table 2). Finally, the traffic collator sub-module verifies the status of stage 1 and stage 2 traffic analysis and decides whether an MC-MitM attack is occurring, identifies its variant, and then hands over the details of the attack to the alert generator unit.

4) ALERT GENERATOR UNIT

This unit creates alerts in case of security events. It mainly logs the alerts with the MAC address of victims, time, and date of the attack.

B. DETECTION METHODOLOGY

In this section, we illustrate the detection methodology followed by the detection controller of our framework.

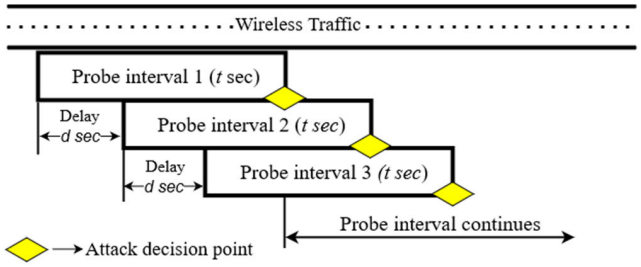


FIGURE 18. Probe interval management.

1) DETECTION LOGIC

The core of the proposed framework's operation is a set of network analysis algorithms that scrutinize filtered and parsed network traffic from the Wi-Fi frame decoder. The detection controller orchestrates the entire detection process using a probe interval structured as a sliding window [61] as shown in Figure 18. Each probe interval duration lasts up to t seconds. Conversely, the second probe interval starts with a delay of d seconds (referred to as the inter-probe interval delay) after the initiation of the first probe interval. Similarly, the third probe interval commences after a lapse of d seconds from the beginning of the second interval, and so forth. This sliding window mechanism serves to ensure that even if an MC-MitM attack fails to breach the predefined thresholds during a specific probe interval, subsequent intervals are still capable of detecting such attacks. This approach allows our framework to maintain continuous monitoring and make determinations about potential attacks every d second, beginning immediately after the first probe interval.

Figure 19 illustrates the overall attack detection logic in a probe interval. The controller module invokes the stage 1 and stage 2 traffic analyzers, which host specific algorithms to detect respective attack signatures. The detection logic comprises 11 algorithms (see Appendix A). Algorithms 1, 2, and 3 belong to the stage 1 traffic analyzer, while algorithms 4, 5, 6, 7, and 8 belong to the stage 2 traffic analyzer. Algorithms 9 and 10, respectively, determine whether the analyzed traffic is malicious or not based on the threshold values (see Table 2). Finally, algorithm 11 acts as a traffic collator that decides on the presence of MC-MitM attacks at the end of each probe interval.

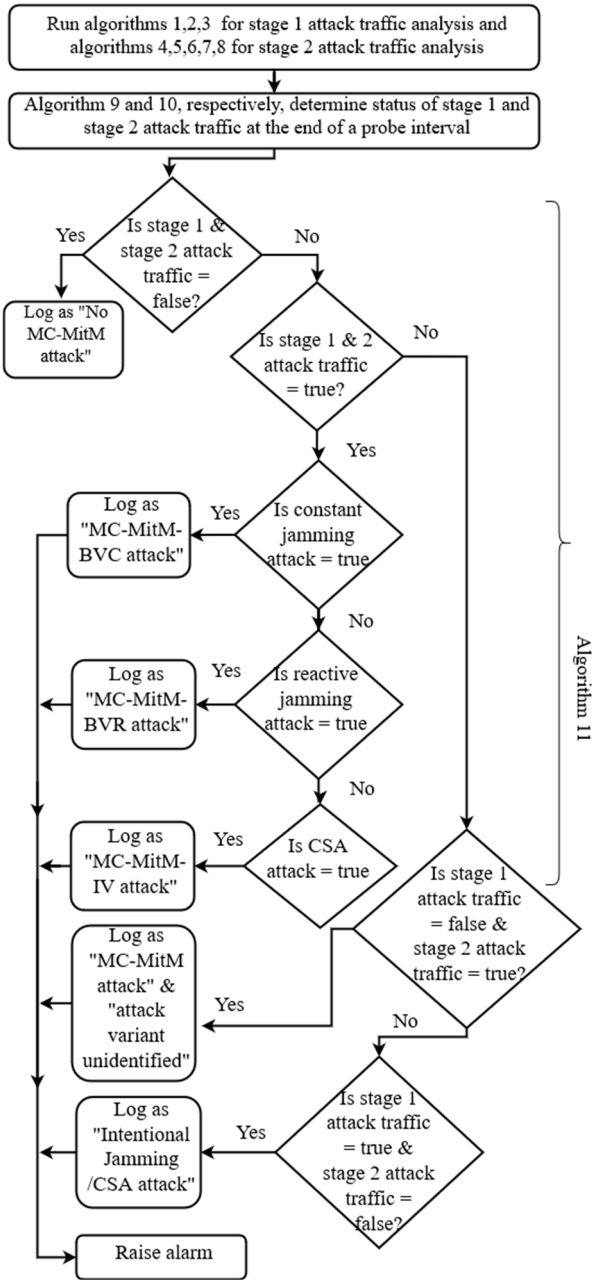


FIGURE 19. Overall detection logic in a probe interval.

VI. EVALUATION

This section is dedicated to the evaluation of the proposed signature-based wireless intrusion detection system (SWIDS) framework for detecting MC-MitM attacks in a representative set of scenarios, with a particular emphasis on personal networks, while still being applicable to enterprise networks.

A. FRAMEWORK IMPLEMENTATION

Our proposed SWIDS framework, outlined in Figure 17, consists of four units implemented in Python. The traffic interceptor unit utilizes different wireless interfaces: TL-WN722N for 2.4 GHz and Wi-Fi Nation for 5 GHz, chosen for cost-effectiveness and monitor mode support across Linux distributions. The device database and MC-MitM detection coordination units use the Scapy libraries to process network packets. Additionally, we incorporated a log file feature to facilitate the tracking of alerts generated by our framework. In this paper, we present the proof of concept (PoC) of our framework implemented on a laptop with Kali Linux OS and is made available in [27].

B. EXPERIMENTAL METHODOLOGY

We conducted our experiment in a practical smart-home environment having an area of approximately 100 sq.m

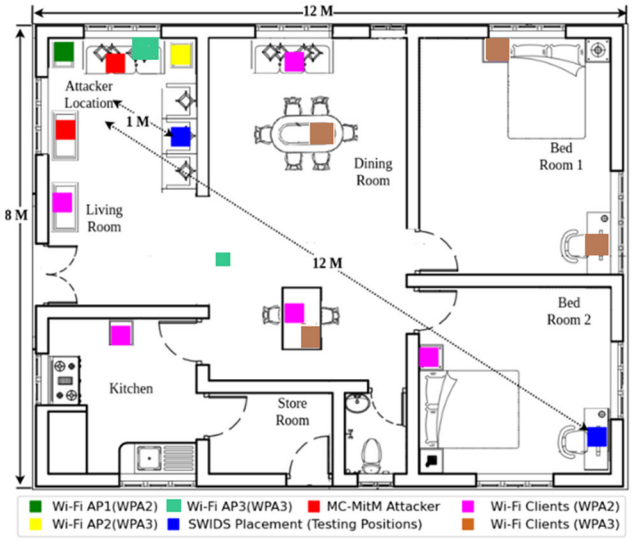


FIGURE 20. Experimental testbed.

(square meter). We employed 15 devices: 3 APs, 9 client devices, 2 attacker devices, and 1 SWIDS device (details of devices used are provided in Table 3). A mixed-mode Wi-Fi network encompassing both WPA2 and WPA3 standards was deployed to accommodate a diverse range of heterogeneous client devices. We connected 5 WPA2 compatible Wi-Fi clients to AP1 and 2 WPA3 compatible client to AP2, and 2 WPA3 compatible client to AP3. For the attackers, we used 2 laptops: one to conduct MC-MitM-IV attacks and another for MC-MitM-BVC or MC-MitM-BVR attacks. The system's performance was evaluated by placing the SWIDs device at two different locations: 1 meter away and 12 meters away from the attacker's location. These locations were chosen to examine the system's effectiveness at both short and possible long distances within our experimental testbed. Our experimental testbed is shown in Figure 20, which illustrates the placement of test devices.

We first performed a set of experiments with the aim of determining an optimal probe interval duration that achieves a true positive rate (TPR) of 90% or higher, considering factors such as the detection time, which refers to the overall time needed to detect different MC-MitM attacks. These experiments were performed within our experimental testbed under normal network traffic conditions, meaning there was no network congestion, and all devices were connected to their respective routers.

Our SWIDS detector node was placed at varying distances from the attacker's location. Specifically, we conducted a series of 75 tests, comprising 25 tests for each of the three MC-MitM attack variants, at a distance of 1 meter. Additionally, we conducted an equivalent number of 75 tests, with 25 tests allocated to each MC-MitM attack variant, at a distance of 12 meters. The results of this first set of experiments are described in Section VI-C.

Once we had determined the probe interval duration needed to reach the desired 90% TPR, we proceeded with the

TABLE 3. Devices used in the experimental testbed.

Device	Type/Role	Wi-Fi standard
TP-LINK Wireless (802.11 N) Router, Speed-144 Mbps, Channel 1(2 GHz), TX power-25-30 dBm	Wi-Fi AP1	WPA2-PSK
D-Link Wireless AX 1500 (802.11 B/G/N) Wi-Fi 6 Router, Speed- 1200 Mbps, Channel 36 (5 GHz), TX power-14 dBm	Wi-Fi AP2	WPA3-SAE
D-Link Wireless AC 1200 (802.11 B/G/N) Wi-Fi 5 Router, Speed-800 Mbps, Channel 36 (5 GHz), TX power-14-17 dBm	Wi-Fi AP3	WPA3-SAE
Samsung S7-Edge	Wi-Fi client of AP1	WPA2
TP-Link Smart Bulb L510E	IoT sensor (Wi-Fi client of AP1)	WPA2
TP-Link Smart Plug P100	IoT sensor (Wi-Fi client of AP1)	WPA2
TP-Link Smart Plug P100	IoT sensor (Wi-Fi client of AP1)	WPA2
Samsung Smart TV	Wi-Fi client of AP1	WPA2
Samsung S8	Wi-Fi client of AP2	WPA2
iPad Mini	Wi-Fi client of AP2	WPA3
Samsung S22	Wi-Fi client of AP3	WPA3
Dell Inspiron 15 30000 series	Wi-Fi client of AP3	WPA3
Lenovo-Thinkpad	Attacker (MC-MitM-IV)	WPA2/3
Toshiba Portege R500	Attacker (MC-MitM-BVC or MC-MitM-BVR)	WPA2/3
HP Elite 8300 with High Gain TP-Link TL-WN722N/Wi-Fi Nation Wi-Fi adaptors	SWIDS Framework	Any

second set of experiments. In this phase, we aimed at testing how effectively our framework prototype could detect different MC-MitM attack variants at various distances under light and heavy traffic conditions. Following a similar approach to the first set of experiments, we conducted 25 detection tests of each MC-MitM attack variant at a distance of 1 meter and another 25 detections of each MC-MitM attack at a distance of 12 meters from the attacker's location. Further, we conducted these experiments in 2 GHz bands. We recreated the light and heavy traffic scenarios within the experimental testbed in the following manner:

1) LIGHT TRAFFIC SCENARIO

We set up a total of 5 Wi-Fi clients connected to Wi-Fi AP1. Wi-Fi AP1 was configured to support IEEE 802.11n mode, and we set the channel frequency to 2.4 GHz with a channel width of 20MHz. This configuration ensured a bitrate (data rate) of 144 Mbps [62]. During the experiments, the connected clients were engaged in web browsing, video streaming, and social media activities, generating a realistic workload representative of light network usage.

TABLE 4. Metrics summary.

Metric	Description	Method
True positive rate (TPR)	Proportion of correct positives relative to total real positives.	(TP) / (TP + FN)
True negative rate (TNR)	Proportion of correct negatives relative to total real negatives.	TN / (FP + TN)
F1-score	Harmonic mean of positive predictive value (precision) and true positive rates.	2TP / (2TP + FP + FN)

2) HEAVY TRAFFIC SCENARIO

For this scenario we utilized a total of 3 Wi-Fi clients connected to Wi-Fi AP1. To create a large volume of wireless traffic, we downloaded large Blu-ray files using P2P connected clients. In addition, we employed the *iperf* tool [63] to generate a maximum bitrate of 100 Mbps. It was ensured that the overall bitrate consistently saturated the channel bandwidth by exceeding 90% during the experiments. The results of this second set of experiments are presented in Section VI-D.

In our third set of experiments, we assess the detection performance of our framework in modern Wi-Fi routers, such as 802.11ac (Wi-Fi AP2) and 802.11ax (Wi-Fi AP3). This evaluation is particularly focused on examining the effects of various channel widths as well as effects of primary and secondary channels. We primarily conducted such experiments in 5 GHz bands. Primary and secondary channels in 5 GHz serve the purpose of optimizing spectrum utilization and minimizing interference, in accordance with the regulatory standards set by each country. In these experiments as well, we conducted 25 detection tests of each MC-MitM attack variant at a distance of 1 meter and another 25 detections of each MC-MitM attack at a distance of 12 meters from the attacker's location, all under light or normal traffic conditions. The results of this second set of experiments are presented in Section VI-E.

In our fourth and final set of experiments, we evaluate performance of our proposed SWIDS framework in terms of CPU and memory utilization. The results of this set of experiments are presented in Section VI-F.

To evaluate the performance capabilities of our framework, we examined the alarm or attack detection status in each experiment by analysing the log file generated by our SWIDS framework. We utilized various metrics as summarized in Table 4. The classification of each prediction result in our framework was based on the following categories: true positive (TP), when an alarm is correctly raised during an attack; true negative (TN), when no alarm is generated in the absence of no attack; false positive (FP), when an alarm is raised erroneously in the absence of an attack; or false negative (FN), when no alarm is generated during an actual attack.

C. RESULTS AND DISCUSSION OF THE FIRST SET OF EXPERIMENTS

In this section, we present the results obtained from our first set of experiments aimed at determining the appropriate probe interval duration and the corresponding detection time for MC-MitM attacks within the experimental testbed.

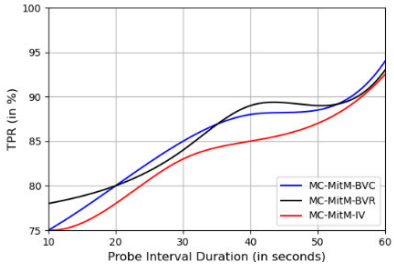


FIGURE 21. Average TPR observed from equal number of detection tests conducted at 1-meter and 12-meter distances under different probe interval duration.

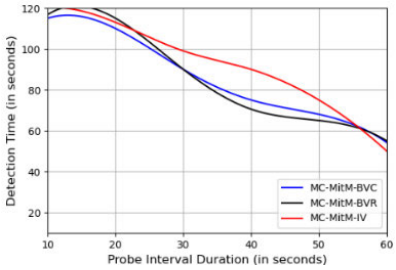


FIGURE 22. Average detection time observed from equal number of detection tests conducted at 1-meter and 12-meter distances under different probe interval duration.

In Figure 21, we illustrate the average TPR as a function of the probe interval duration for the three types of MC-MitM attacks, including the base variant attacks (MC-MitM-BVC and MC-MitM-BVR) as well as improved variant attack (MC-MitM-IV). As seen from Figure 21, we can observe that our framework achieves an average TPR exceeding 93% when employing a probe interval of 60 seconds. This is because, with a probe interval of 60 seconds, our framework collects a sufficient amount of attack frames and data to potentially distinguish different MC-MitM attacks and their variants. This also highlights the superior performance of our algorithms when longer observation times are employed.

In Figure 22, we illustrate the average detection time (time delay to detect different MC-MitM attacks) at 1-meter and 12-meter distances. As seen from Figure 22, we can observe that the detection time decreases as the probe interval increases due to the availability of a larger pool of attack data. Specifically, when the probe interval duration is set to 60 seconds, our framework achieves an average detection time of 50-55 seconds. This indicates an average improvement of 45-50% in the detection time compared to a probe interval duration of 10 seconds.

Since the 60 seconds probe interval duration allows our framework to achieve the desired TPR with a considerable low detection time, we have adopted this duration for all subsequent experiments in our framework. Additionally, based on our experiments where we observed a significant improvement in detection performance with a 10 seconds inter-probe

delay (d seconds in Figure 18), we have configured the inter-probe interval delay to 10 seconds in our detection logic to reduce the chances of missed attacks.

The values we have obtained for t and d can be applied to other environments with different hardware settings, and we can assure that the detection results obtained will remain equally acceptable (TPR $>$ 90%). This is due to the high detection capacity of stage 2. Even when the attack traffic in stage 1 lasts for a long time, usually as a result of reactive jamming attacks, the attack is swiftly detected in stage 2, because the thresholds in this stage are equal to one and, therefore, concurrent traffic is detected almost instantaneously. Consequently, by employing a probe interval of 60 seconds and an inter-probe delay of 10 seconds, we maximize the detection possibilities of stage 1, and when this stage fails and the specific type of attack cannot be determined, the alarm is triggered in stage 2 and the attack variant is marked as ''unidentified''. The last outcome can be caused by long reactive jamming attacks or a high packet loss ratio.

D. RESULTS AND DISCUSSION OF THE SECOND SET OF EXPERIMENTS

In this section, we present the results obtained from our second set of experiments, which aimed to evaluate the performance of the SWIDS framework in detecting various MC-MitM attacks under both light and heavy traffic scenarios. These experiments were conducted to assess the effectiveness and reliability of the SWIDS framework in real-world network environments with different traffic conditions.

In. Figure 23, we show the detection performance achieved under light and heavy traffic scenarios at a short-distance (1 meter) and long-distance (12 meters) from the attacker's location. As seen from Figure 23, our proposed framework demonstrates the capability to detect different MC-MitM attack variants with a minimum TPR of 83% at 1-meter distance and 70% at 12-meter distance under various traffic scenarios. Among the results, the detection of MC-MitM-BVC (see Figure 23(a) and (b)) and MC-MitM-BVR (see Figure 23(c) and (d)) attacks exhibits the most favorable performance. This can be attributed to the effectiveness of our framework's stage 1 attack traffic detection. In the case of MC-MitM-BVC attacks, constant jamming results in abrupt changes in the corresponding FIAT and FDR values, which our framework can promptly detect even at longer distances and under heavy traffic scenarios. Similarly, reactive jamming employed in MC-MitM-BVR attacks induces many malformed frames, which provide sufficient evidence for our framework to detect such attacks during specific probe intervals. However, the detection of MC-MitM attacks presents some challenges. In certain instances of MC-MitM-IV attacks, fake CSA attacks remain undetected as there are only a few CSAs (4 CSA beacons as per standards) in an attack, which may be lost or dropped during detection. This is mainly observed at 12 meters and in heavy traffic scenarios (see Figure 23(f)).

Moreover, the stage 2 attack introduces frame loss, especially in the case of concurrent connection establishment traffic, since such traffic consists of fewer frames (2 authentication, 2 associations, and 4 EAPOL frames) than concurrent beacon/probe response and concurrent data traffic. Consequently, the detection of all MC-MitM attack variants is affected.

The decrease in the obtained TPR at longer sensing distances can be primarily attributed to an increased frame loss rate experienced by our framework during different probe intervals. Frame loss can occur due to the network conditions, parsing and processing time for each frame, and the processing power of the Wi-Fi cards. Consequently, our framework may misclassify a certain fraction of attacks as benign traffic (see Figure 23(d), (e), and (f)).

Due to the frame loss at distances of 12 meters or under heavy traffic scenarios, stage 1 attack traffic remains undetected in a few cases. Yet, our framework successfully detected MC-MitM attacks that involved a combination of concurrent beacon/probe response traffic with concurrent connection establishment traffic or concurrent data traffic. However, identifying the specific attack variants in such cases proved challenging, resulting in an average of 3% of uncategorized MC-MitM attacks during our experiments.

Regarding the performance difference between light and heavy traffic scenarios, our framework exhibits good performance under both scenarios at 1-meter distances, with only an average 5% drop in detection accuracy under heavy traffic scenarios compared to light traffic scenarios. However, at a distance of 12 meters, there is an average performance drop of 14% under heavy traffic scenarios. This is because, frame loss is more prevalent at long distances.

Furthermore, our framework shows good confidence in correctly distinguishing attacks, with 100% TNR in all test scenarios. As a consequence, there are also no false positives (although not explicitly shown in Figure 23) as we used predefined rules to identify the signatures of stage 1 and stage 2 traffic during MC-MitM attacks. Finally, our framework maintained reasonable F1-scores (above 82%) in all test scenarios.

E. RESULTS AND DISCUSSION OF THE THIRD SET OF EXPERIMENTS

In this section, we provide the outcomes of our third set of experiments. These experiments were conducted to assess the performance of our SWIDS framework in the detection of various MC-MitM attacks across varying channel bandwidths, and primary and secondary channels in the 5 GHz bands of modern Wi-Fi networks. Furthermore, the evaluation covered a different detector location from the attacker.

In Figure 24, we show the average TPR while detecting different MC-MitM attacks under each different channel bandwidths of the Wi-Fi AP2 (802.11ac) and Wi-Fi AP3 (802.11ax) as specified in Table 3, from detection tests conducted at 1-meter and 12-meter distances from the attacker location. As shown in Figure 24 (a) and (b), we can see that

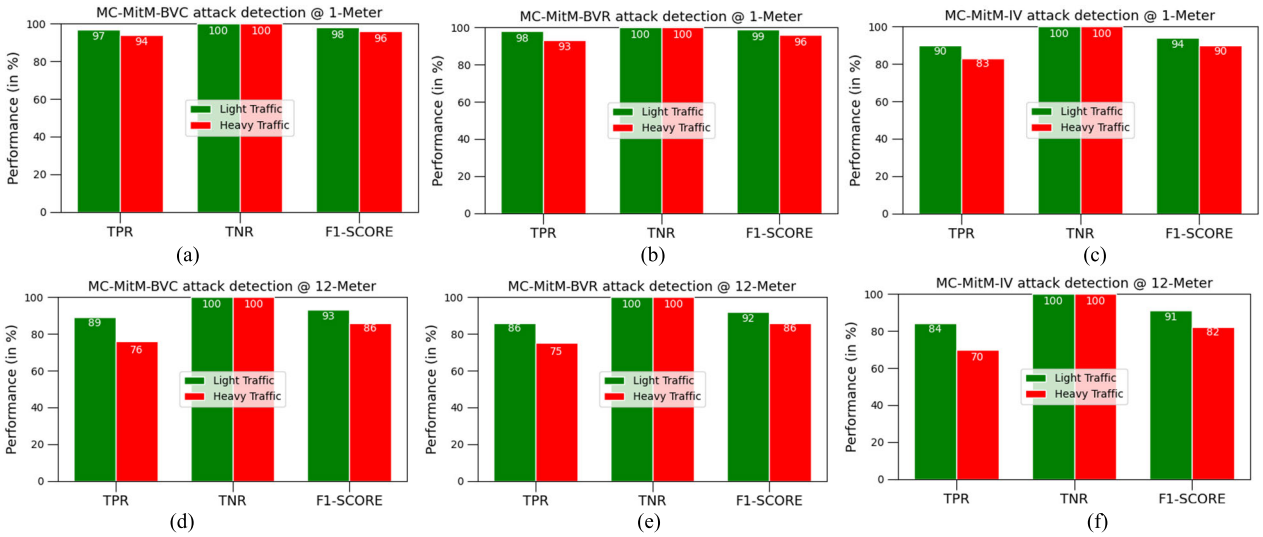


FIGURE 23. Detection performance achieved under light and heavy traffic scenarios with (a) MC-MitM-BVC at 1-meter; (b) MC-MitM-BVR at 1-meter; (c) MC-MitM-IV at 1-meter; (d) MC-MitM-BVC at 12-meter; (e) MC-MitM-BVR at 12-meter, and (f) MC-MitM-IV at 12-meter.

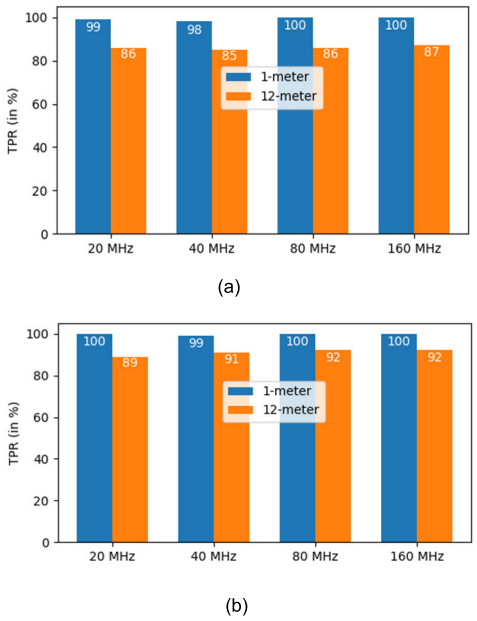


FIGURE 24. Average TPR observed under different channel bandwidths at 1-meter and 12-meter distances (a) with 802.11ac networks; (b) with 802.11ax networks.

our SWIDS framework effectively detect various MC-MitM attack variants, achieving an average TPR of up to 99% in both 802.11ac and 802.11ax networks at a 1-meter distance.

At a 12-meter distance, the TPR averages at 86% for 802.11ac and 91% for 802.11ax networks. This signifies a decline in TPR, about 13% for 802.11ac and 8% for 802.11ax, when comparing the 1-meter and 12-meter distances. This clearly demonstrates that distance of detector from the attacker is the primary factor influencing the performance of our framework. On the other hand, the detection performance remains relatively consistent across all channel bandwidths of both 802.11ac and 802.11ax networks.

This is because, as per standards, the maximum transmitted power (e.g., 14 dBm in our experiments) set in an AP remains constant regardless of the channel bandwidth [63], [64], which mainly affect the reception of frames by our detector. While this high transmit power enables Wi-Fi frames to cover extended distances, it results in a lower Received Signal Strength Indicator (RSSI) when these frames encounter obstacles such as walls in a home or buildings, leading to potential frame loss. Therefore, it becomes apparent that a wider channel bandwidth does not significantly impact our framework's detection performance.

In Figure 25, we show the average TPR while detecting different MC-MitM attacks across primary and secondary channels (any adjacent channel) under each different channel bandwidths. These results stem from an equal number of detection tests conducted in both 802.11ac and 802.11ax networks. Additionally, the evaluation considered different detector locations from the attacker.

In the context of our channel experiments, we chose commonly used non-overlapping channels to minimize the potential for interference from adjacent networks. Specifically, we selected primary and secondary channel pairs as follows: 36 and 40 for 20 MHz, 36 and 44 for 40 MHz, 36 and 52 for 80 MHz, and 36 and 100 for 160 MHz [64], [65] both in 802.11 ac and 802.11ax networks.

As shown in Figure 25 (a), we can see that our SWIDS framework effectively detect various MC-MitM attack variants with an average TPR exceeding 97% in both primary and secondary channels across different channel bandwidths at a 1-meter distance.

Similarly, at a 12-meter distance, our framework maintains an average TPR of at least 85% in both primary and secondary channels, regardless of the channel bandwidth. Furthermore,

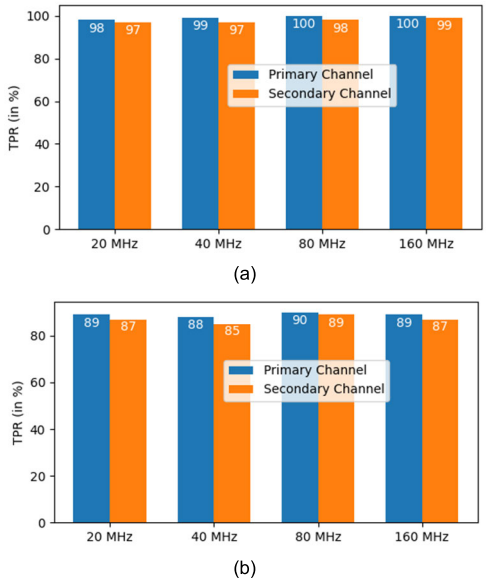


FIGURE 25. Average TPR observed under primary and secondary channels of different channel bandwidths in both 802.11ac and ax networks at: (a) 1-meter; (b) 12-meter distances.

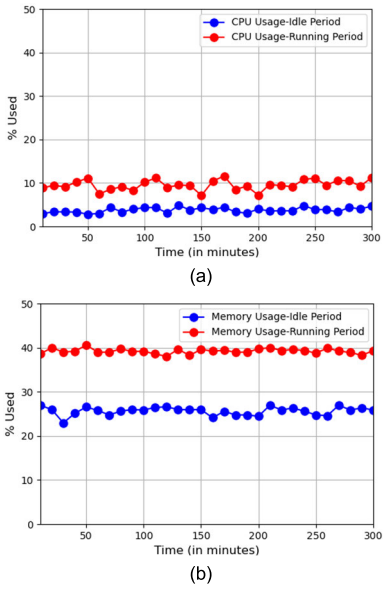


FIGURE 26. Performance overhead of SWIDS framework in terms of (a) CPU usage; (b) Memory usage.

in Figure 25 (a) and (b), it is evident that there is a decrease in detection performance of approximately 11-12% when comparing a 1-meter distance to a 12-meter distance. This further reinforces our findings that distance is the primary factor influencing the detection performance. Consistent with our previous experiments, it is evident from Figure 25 (a) and (b) that the detection performance remains relatively stable across various channel bandwidths. This indicates that the choice of the operating channel in Wi-Fi also does not significantly impact our framework's ability to detect MC-MitM attacks.

Finally, from Figures 24 and 25, we conclude that the primary factor contributing to the performance drop lies in frame loss due to the distance between the detector and attacker locations or frame processing delays within our SWIDS framework. Additionally, network conditions and environmental factors, including traffic volume, building materials, and network overhead, contribute to reduced wireless signal range and throughput. These experiments further reinforce the findings presented in Section VI-D. Nevertheless, our framework exhibits relatively good detection performance, particularly in modern 802.11ax or Wi-Fi 6 enabled networks. This improvement is attributed to the increased Received Signal Strength Indicator (RSSI) in wireless frames received at our detectors as well as improved transmission features and throughput.

F. RESULTS AND DISCUSSION OF THE FOURTH SET OF EXPERIMENTS

In order to test the performance overhead of our proposed defense mechanism in terms of CPU and memory utilization, we conducted an experiment on a Kali Linux laptop (Intel core i3 with 4GB RAM) hosted with our proposed defense mechanism. More specifically, we measured how much CPU and memory were used in the previous N minutes (in our case, we used 300 minutes) by our SWIDS framework during its idle and running periods (see Figure. 26).

As shown in Figure 26 (a), we can observe that the CPU usage increases by an average of only 5% when SWIDS framework is active, which can be primarily attributed to Wi-Fi frame capture and subsequent extraction procedures. Regarding memory consumption (see Figure 26(b)), when our SWIDS framework is active, there is merely a 12% average increase (0.48GB). This is because the defense mechanism stores solely the quantity of malicious frames and the status of the corresponding attack traffic during each probe interval duration.

The efficiency of the proposed framework becomes evident with the aforementioned results. It qualifies as a lightweight solution ideal for low-cost devices like a Raspberry Pi 4 with 8GB of RAM and featuring a quad-core cortex-a72 processor[2], which has a performance of 20% of an Intel Core i3-7100. Note that in a raspberry pi 4, SWIDS would consume around 25% of the CPU and 6% of the RAM.

G. COMPARISON WITH EXISTING DEFENSE MECHANISMS

In this section, we compare our proposed SWIDS framework with existing state-of-the-art defense mechanisms, particularly stage 1 defense mechanisms (see Section II-B.1) since they identify the root causes or attack vectors for MC-MitM attacks.

[2]Comparison of the performance of a single-thread CPU arm-cortex-a72 vs intel-core-i3-7100 https://versus.com/en/arm-cortex-a72-vs-intel-core-i3-7100

TABLE 5. Comparison of SWIDS with exisiting defense mechanisms.

Defense mechanism/ Metrics	Detect MC-MitM attack against WPA2/3 clients	Detect MC-MitM attack against PMF capable /incapable clients	Detect insider/outsider MC-MitM attacks	Provides detection and/or prevention of MC-MitM attacks	Recognize MC-MitM attack variant	Mandates Protocol changes/ Integration of software/ hardware /no changes	Provides backward compatibility
Proposed SWIDS framework	○	○	○	□	○	○	○
OCV [34]	■	□	○	○	■	□	■
Beacon Protection [16]	■	□	■	○	■	□	■
Stupify [37]	□	■	■	□	■	□	■
SSAD [19]	□	■	○	□	■	■	■
SAE-PK [35]	■	□	■	○	■	□	■

We do not consider stage 2 defense mechanisms since they focus only on detecting or preventing specific attacks (e.g., KRACK) using MC-MitM positions. Further, for comparison purposes, we consider various metrics, such as: (1) whether the defense mechanism detects MC-MitM attacks against WPA/2 clients (□), WPA3 clients (■), or both (◯); (2) whether the defense mechanism detects MC-MitM attacks against PMF capable clients (□), against PMF incapable clients (■), or both (◯); (3) whether the defense mechanism detects insider MC-MitM attacks (□), detects outsider MC-MitM attacks (■), or both (◯); (4) whether the defense mechanism provides detection only (□) or both detection and prevention (◯) of MC-MitM attacks; (5) whether the defense mechanism detects or recognizes all MC-MitM attack variants (◯) or not (■); (6) whether the defense mechanism requires any protocol or firmware modification (□), integration of software/hardware (■), or no changes (◯) for its deployment and (7) whether the defense mechanism provides backward compatibility to safeguard old or outdated devices (◯) or not (■) from MC-MitM attacks. The comparison is illustrated in Table 5. The more open circles (i.e., icon ◯) are shown in the row of a particular defense mechanism, the more effective the defense mechanism is for detection of MC-MitM attacks.

According to Table 5, OCV [34] and Beacon Protection [16] defense mechanisms detect and prevent MC-MitM attacks. However, these mechanisms are currently only available with WPA3 devices or PMF-enabled devices, since they have only recently been included in the WPA3 standards. Regarding the detection of insider/outsider attacks, while OCV effectively identifies both of these attacks as it checks for unauthorized communication channels during a 4-way handshake process, the Beacon Protection mechanism cannot detect insider attacks because attackers can forge legitimate beacons. Although the above mechanisms detect the presence of MC-MitM attacks, they cannot correctly identify which specific attack variant is being used.

Stupify [37] only detects attacks against WPA2 devices because it introduces changes to the WPA2 authentication mechanisms. It does not protect PMF devices as they do not include a group key (IGTK) in their authentication mechanism, and cannot detect insider attacks since such attackers can forge/bypass authentication details. Similarly, SSAD [19] can only detect and prevent attacks against WPA/2 devices because it introduces a new patch for wpa_supplicant for the WPA2 standards. It can also detect attacks against PMF devices and identifies insider and outsider attacks as they passively monitor for multiple beacons with the same combination of SSID and BSSID. However, SSAD only identifies base variant (MC-MitM-BV) attacks, not improved variant (MC-MitM-IV) attacks because it cannot recognize fake CSAs.

SAE-PK [35] protects only PMF-capable or WPA3 clients using SAE authentication and mainly aims at defending against insider attacks, especially in public Wi-Fi networks. However, MC-MitM attackers can bypass this defense (see Section II-B.1). Also, SAE-PK is not able to distinguish between MC-MitM attack variants.

From an implementation standpoint, all existing defense mechanisms require complex firmware updates or hardware/software integration across all Wi-Fi devices, which is impractical, especially in IoT networks. Finally, none of the existing defense mechanisms are backward compatible with old or obsolete devices.

Contrastingly, our proposed SWIDS framework is a plug-and-play system that passively monitors specific signatures of MC-MitM attacks. It has a very low complexity that can be easily operated by a common user, and can be easily integrated into any Wi-Fi or IoT environment to detect attacks against all kinds of devices in a WPA2/3 network, including PMF-capable devices. Our SWIDS framework can also effectively defend against insider and outsider attacks and different MC-MitM attack variants. In addition, our SWIDS is backward compatible with old or legacy devices and is easy to use, as it does not require any protocol or device modifications on each Wi-Fi client and/or AP. Therefore, from the comparison in Table 5, we can state that our SWIDS outperforms the existing defense mechanisms and is a generalizable defense with improved security against MC-MitM attacks.

H. DISCUSSION ON EXISTING SIGNIFICANT DATASETS

The AWID3 dataset [26] is widely utilized as a publicly available dataset for studying various Wi-Fi attacks. It includes multiple attack traces stored as PCAP files,

TABLE 6. Comparison of performance in identifying/classifying Krack attacks from AWID3 dataset.

Reference	F1 Score	Accuracy	Detection Type
[45] Table 17	-	98.69	ML based
[44] Table 4	88.07	98.73	ML based
[46] Table 1	90.17	90.15	ML based
[43] Table 4	98.51	98.50	ML based
Proposed SWIDS framework	99.08	100	Threshold Based

including instances of KRACK attacks. However, when considering the detection of MC-MitM attacks, the AWID3 dataset can only be used to identify KRACK attacks, which are just one type of MC-MitM enabled attacks. Therefore, the AWID3 dataset is not a generalizable dataset to correctly distinguish all types of MC-MitM attacks. In contrast, as detailed in Section IV-D, we have created our own dataset that includes traffic from the different types of MC-MitM attacks and their variants. This dataset has been used to define our own attack signatures, which have been later used in the experiments described in Section VI-B to evaluate our framework's performance.

We also tested our SWIDS framework using the external AWID3 dataset. To evaluate the performance of our framework in detecting KRACK signatures, we input the AWID3 PCAP file directly into the Traffic Interceptor Unit of our framework (see Figure 17), instead of performing online monitoring or passive capturing. We employed our proposed signatures to detect KRACK behavior in this dataset and we successfully identified the retransmission of message 3 of the 4-way handshake, a behavior that signals the presence of MC-MitM attacks, occurring across multiple channels (channel 2 and 13). Thus, our SWIDS framework effectively detected retransmitted handshake messages in this scenario. In Table 6, we present a performance comparison (F1 Score and/or accuracy, whichever available) of existing detection mechanisms that make use of publicly available AWID3 dataset to identify KRACK attacks.

As we can see from Table 6, the F1 Score and accuracy achieved by our proposed SWIDS framework is higher than in other proposals that utilize the AWID3 dataset. This is because our framework exhibits minimal instances of undetected attack frames. The undetected attacks can be attributed to slight delays in frame processing during the attack detection process. This also demonstrates that our proposed SWIDS framework is adequate to accurately detect the presence of MC-MitM attacks.

We must bear in mind, however, that our proposal is based on real-time detection, whereas the methods reviewed in this section are based on offline analysis of network data using machine learning algorithms. Therefore, the results of our framework are those shown in Section VI-D. Here, we have shown the result of feeding the AWID3 data into our Traffic Interceptor Unit just for comparative purposes.

I. SECURITY CONSIDERATIONS

Our SWIDS framework is the first of its kind to identify MC-MitM attacks and is applicable to all Wi-Fi networks and devices. Since our framework passively monitors Wi-Fi networks, it can identify both insider and outsider threats against any type of Wi-Fi device. Moreover, our framework is difficult for an attacker to circumvent, even if he is aware of the deployed defense mechanisms and algorithms used. This is due to the fact that we defined the thresholds for identifying the appearance of malicious frames as part of the essential operations (stage 1 and stage 2 attack traffic) required for successful MC-MitM attacks, and it is impossible to carry out such attacks without meeting or surpassing those thresholds. Furthermore, even if the attacker devises any other new tactics to deceive the victim besides jamming or CSA attacks as part of stage 1 traffic, the stage 2 traffic remains visible to our SWIDS. Lastly, our framework follows a plug-and-play deployment and does not require any protocol or device modifications on Wi-Fi clients and/or AP. Thus, standard users will be able to set up our proposed defense mechanism with significantly less technical difficulty.

J. LIMITATIONS OF OUR FRAMEWORK

While our SWIDS framework is versatile and applicable to both personal and enterprise networks, it currently monitors a single AP/single Wi-Fi network at a time. This design choice aligns with the nature of MC-MitM attacks, which typically target one AP at a time, focusing on specific SSID, BSSID, and operating channels. As of now, our framework does not support concurrent monitoring of two APs or different channels, such as 2.4 GHz and 5 GHz. We also indicate that our current framework is focused on detecting MC-MitM attacks and does not include prevention capabilities. However, our future work involves addressing these limitations by developing a distributed detection system that will enable multiple detectors to concentrate on different APs with varying channel frequencies, thereby enhancing the framework's detection capabilities.

VII. CONCLUSION AND FUTURE WORKS

In this paper, we highlighted the capabilities and impact of MC-MitM attacks on Wi-Fi networks. We described various challenges posed by MC-MitM attacks regarding effective detection and implementation difficulties of existing defense mechanisms. To this end, we proposed a lightweight signature-based intrusion detection system framework to detect different MC-MitM attack variants. We first classified and investigated network traffic behavior during MC-MitM attacks. We then designed attack signatures and identified useful metrics to detect MC-MitM attacks through various theoretical and empirical analyses of the attack and benign traffic behavior. From these signatures, we created detection algorithms for identifying different MC-MitM attack variants. We then implemented our framework using scapy, a python library for packet capturing and manipulation, and

commercially available wireless interfaces. Our framework is a centralized, passive monitoring system that can be easily integrated with Wi-Fi-based IoT environments. Further, our framework is independent of any Wi-Fi protocols or standards, does not require modifying existing network settings or device modifications, and provides continuous security against MC-MitM attacks

We then evaluated our framework with real MC-MitM attacks in an experimental IoT network setup and specifically analyzed detection performance at different distances. We found that our framework exhibits a minimum TPR of 90% using short-distance detectors and 84% using long-distance detectors with a detection delay of maximum 60 seconds. In addition, we analyzed performance of our framework under various channels and channel bandwidths. We showed that the choice of any specific channel or channel bandwidth does not significantly impact our framework's detection performance. We also showed that our SWIDS framework incurs minimal overhead in terms of CPU and memory usage. These results emphasize the versatility of our detection logic, suggesting its applicability to diverse smart home network contexts.

We also showed that frame loss affects detection performance with long-distance detectors, especially in 2.4 and 5 GHz bands. Based on our evaluation, we plan to extend the present framework to include a distributed and cooperative intrusion detection system to enhance performance in our future works. Specifically, our intention is to deploy this implementation on single-board computers, such as Raspberry Pis, which are commonly used for various smart home applications like Home Assistants or OpenHAB. This approach will not only reduce the cost-effectiveness of our framework but also enable its evaluation in wide-ranging practical Wi-Fi based IoT environments hosting multiple APs.

APPENDIX A
NETWORK ANALYSIS ALGORITHMS

In this Appendix, we briefly discuss various network analysis algorithms and their operations.

A. ALGORITHM 1: CONSTANT JAMMING ANALYSIS

During a probe interval, this algorithm computes: (1) an array of FIAT, where each FIAT is measured from two successive beacons; (2) total number of beacons captured on the legitimate channel of the AP.

Algorithm 1 Constant Jamming Analysis (Detect Constant Jamming Behavior)

```
Data: Wireless traffic
Result: Array of FIAT (A-FIAT), Number of beacons (NB)
while probe-interval do
    Calculate FIAT between two successive beacons; Record each
      FIAT to A-FIAT;
    Count number of beacons(NB);
end
```

B. ALGORITHM 2: MALFORMED FRAME ANALYSIS

This algorithm counts the number of malformed frames due to reactive jamming in a probe interval. This is done by verifying the FCS flags present in the header of the beacon and probe response frames, especially those arriving on the legitimate channel of the AP.

Algorithm 2 Malformed Frame Analysis (Detect Reactive Jamming Behavior)

```
Data: Wireless traffic
Result: Number of malformed frames (MF) AP-MAC=MAC ID of
the AP;
C-CHANNEL=Current channel of the AP;
while probe-interval do
    if frame.haslayer(Dot11) then
        Extract bssid and channel of the frame;
        if bssid == AP-MAC and (frame.haslayer(Dot11Beacon)
          or frame.haslayer(Dot11ProbeResp)) and channel
          ==C-CHANNEL then
            RT = frame.getlayer(RadioTap);
            if RT.Flags == "FCS+badFCS") then
                Count malformed-frame (MF); Store current
                  channel;
            end
        end
    end
end
```

C. ALGORITHM 3: CHANNEL SWITCH ANALYSIS

This algorithm counts the number of beacons, probe responses, or action frames with CSA information elements in the legitimate channel of the AP. Such information elements are extracted from the frames using the tag ID. 37.

Algorithm 3 Channel Switch Analysis (Detect CSAs)

```
Data: Wireless traffic
Result: Number of CSA (CSA) AP-MAC=MAC ID of the AP;
C-CHANNEL=Current channel of the AP;
while probe-interval do
    Extract bssid of the frame;
    if bssid == AP-MAC and (frame.haslayer(Dot11Beacon) or
      frame.haslayer(Dot11ProbeResp) or frame.subtype == 13)
      then
        Extract each Information Element (IE);
        if IE-ID is 37 then
            Count CSA (CSA);
        end
    end
end
```

D. ALGORITHM 4: CONCURRENT BEACON OR PROBE RESPONSE TRAFFIC ANALYSIS

This algorithm simultaneously monitors and counts the beacon or probe response traffic with the targeted SSID and BSSID on the legitimate channel of the AP and those beacon or probe response traffic with the same SSID and BSSID on any other channel (channel hopping) during a probe interval.

Algorithm 4 Concurrent Beacons/Probe Response Traffic Analysis

```
Data: Wireless traffic
Result: Number of concurrent beacons (BCC and BRC)/probe
responses(PCC and PRC)
AP-MAC=MAC ID of the AP, SSID-AP=SSID of the AP;
C-CHANNEL=Current channel of the AP;
while probe-interval do
    Extract ssid,bssid, ad channel of the frame;
    if (frame.haslayer(Dot11Beacon) then
        if bssid == AP-MAC and ssid == SSID-AP and channel
          == C-CHANNEL then
            Count beacon-current-channel(BCC);
        end
        if bssid == AP-MAC and ssid == SSID-AP and (channel
          != C-CHANNEL) then
            Count beacon-rogue-channel(BRC);
        end
    else
        if frame.haslayer(Dot11ProbeResp) then
            if bssid == AP-MAC and ssid == SSID-AP and
              channel == C-CHANNEL then
                Count probe-current-channel(PCC);
            end
            if bssid == AP-MAC and ssid == SSID-AP and
              (channel != C-CHANNEL) then
                Count probe-rogue-channel(PRC);
            end
        end
    end
end
```

E. ALGORITHMS 5, 6, AND 7: CONCURRENT CONNECTION ESTABLISHMENT TRAFFIC ANALYSIS

Similar to algorithm 4, these algorithms simultaneously monitor connection establishment traffic between specific clients and the AP on the legitimate channel and any other channel during a probe interval.

Algorithm 5 Concurrent Authentication Traffic Analysis

```
Data: Wireless Traffic
Result: Number of Concurrent Authentication frames(AUTHCC
and AUTHRC) AP-MAC=MAC ID of the
AP,C-CHANNEL=Current Channel of the AP;
while Probe-interval do
    Extract Smac,dmac,channel of the Frame;
    if frame[Dot11].Type == 0 and frame[Dot11].Subtype == 11
      then
        while Client-Mac in Device database do
            if (smac == AP-MAC and Dmac == Client-Mac) or
              (smac == Client-Mac and Dmac == AP-MAC)
              and Channel == C-CHANNEL then
                Count
                  Authentication-Current-channel(AUTHCC);
            end
            if (smac == AP-MAC and Dmac == Client-Mac) or
              (smac == Client-Mac and Dmac == AP-MAC)
              and Channel != C-CHANNEL) then
                Count Beacon-Rogue-channel(AUTHRC);
            end
        end
    end
end
```

More specifically, algorithm 5 counts concurrent authentication traffic, algorithm 6 counts concurrent association traffic, and algorithm 7 counts concurrent EAPOL traffic. Further, all these algorithms work in parallel and analyse the traffic using the device's source and destination MAC addresses.

Algorithm 6 Concurrent Association Traffic Analysis

```
Data: Wireless traffic
Result: Number of concurrent association frames (ASSOCC and
ASSORC) AP-MAC=MAC ID of the AP,C-CHANNEL=Current
channel of the AP;
while probe-interval do
    Extract smac,dmac,channel of the frame;
    if frame[Dot11].type == 0 and frame[Dot11].subtype == 1
      then
        while client-mac in device database do
            if (smac == AP-MAC and dmac == client-mac) or
              (smac == client-mac and dmac == AP-MAC) and
              channel == C-CHANNEL then
                Count association-current-channel(ASSOCC);
            end
            if (smac == AP-MAC and dmac == client-mac) or
              (smac == client-mac and dmac == AP-MAC) and
              channel != C-CHANNEL) then
                Count association-rogue-channel(ASSORC);
            end
        end
    end
end
```

Algorithm 7 Concurrent EAPOL Traffic Analysis

```
Data: Wireless traffic
Result: Number of EAPOL frames (EAPOLCC and EAPOLRC)
AP-MAC=MAC ID of the AP,C-CHANNEL=Current channel of
the AP;
while probe-interval do
    Extract smac,dmac,channel of the frame;
    if frame.haslayer(EAPOL) and (frame[Dot11].type != 1 then
        while client-mac in device database do
            if (smac == AP-MAC and dmac == client-mac) or
              (smac == client-mac and dmac == AP-MAC) and
              channel == C-CHANNEL then
                Count EAPOL-current-channel(EAPOLCC);
            end
            if (smac == AP-MAC and dmac == client-mac) or
              (smac == client-mac and dmac == AP-MAC) and
              channel != C-CHANNEL) then
                Count EAPOL-rogue-channel(EAPOLRC);
            end
        end
    end
end
```

F. ALGORITHMS 8: CONCURRENT DATA TRAFFIC ANALYSIS

This algorithm monitors and counts concurrent data traffic following the concurrent connection establishment traffic.

Algorithm 8 Concurrent Data Traffic Analysis

```
Data: Wireless traffic
Result: Number of data frames (DATACC and DATARC)
AP-MAC=MAC ID of the AP,C-CHANNEL=Current channel of
  the AP;
while probe-interval do
    Extract smac,dmac,channel of the frame;
    if frame[Dot11].subtype == 32 and frame[Dot11].subtype
      == 40 then
        while client-mac in device database do
            if (smac == AP-MAC and dmac == client-mac) or
              (smac == client-mac and dmac == AP-MAC) and
              channel == C-CHANNEL then
                Count data-current-channel(DATACC);
            end
            if (smac == AP-MAC and dmac == client-mac) or
              (smac == client-mac and dmac == AP-MAC) and
              channel != C-CHANNEL) then
                Count data-rogue-channel(DATARC);
            end
        end
    end
end
```

G. ALGORITHM 9: MC-MITM STAGE 1 ATTACK TRAFFIC COLLATOR

At the end of the first sub-probe interval, this algorithm: (1) calculates the overall FIAT from the standard deviation of the FIAT values and the FDR from the number of beacons received during the probe interval, as provided by algorithm 1; (2) calculates malformed rate (MF-rate) from the number of malformed frames provided by algorithm 2 and (3) obtains the number of CSAs from algorithm 3. Based on the threshold values (see Table 2) of these stage 1 attack traffic, algorithm 4 determines whether the stage 1 attack traffic is dubious or not.

Algorithm 9 MC-MitM Stage 1 Attack Traffic Collator

```
Data: Output of Algorithms 1,2 and 3
Result: Status of stage 1 attack traffic
FIAT =SD(A-FIAT),FDR=(NB/600)*100, MF-rate=
  (MF/60)*100;
if (FIAT≤ TH1 and FDR≤ TH2 and MF− rate≤ TH3 and CSA <
  TH4) then
    STAGE-1-ATTACK-TRAFFIC = False;
else
    if (FIAT≥ TH1 and FDR≥ TH2)) then
        CONST-JAM-ATTACK = True;
        LOG as "Intentional jamming attack";
    end
    if (MF− rate≥ TH3) then
        REACTIVE-JAM-ATTACK = True;
        LOG as "Intentional jamming attack";
    end
    if ((CSA≥ TH4) then
        CSA-ATTACK = True;
        LOG as "CSA attack";
    end
end
```

H. ALGORITHM 10: MC-MITM STAGE 2 ATTACK TRAFFIC COLLATOR

This algorithm determines the status of the stage 2 attack traffic at the end of every probe interval based on threshold values (see Table 2).

Algorithm 10 MC-MitM Stage 2 Attack Traffic Collator

```
Data: Output of Algorithms 4, 5, 6, 7 and 8
Result: Status of Stage 2 Attack Traffic
if (BRC == 0 and AUTHRC == 0 and ASSORC == 0 and
  EAPOLRC == 0 and DATARC == 0) then
    STAGE-2-ATTACK-TRAFFIC = False;
else
    if (BCC≥ TH5 and BRC≥ TH5 and PCC≥ TH5 and PRC≥
      TH5) then
        CON-BEACON-PROBE = True;
    end
    if (AUTHCC≥ TH6 and AUTHRC≥ TH6 or ASSOCC≥ TH6
      and ASSORC TH6 or EAPOLCC TH7 and EAPOLRC TH7)
      then
        CON-CONNECTION-EST = True
    end
    if (DATACC TH8 and DATARC TH8) then
        CON-DATA = True
    end
    if (CON-BEACON-PROBE = True and
      (CON-CONNECTION-EST = True or CON-DATA = True))
      then
        STAGE-2-ATTACK-TRAFFIC = True;
    else
        STAGE-2-ATTACK-TRAFFIC = False;
    end
end
```

I. ALGORITHM 11: ALARM GENERATION

Based on the status of stage 1 and stage 2 attack traffic provided by algorithms 9 and 10, algorithm 11 predicts the presence of MC-MitM attacks and variants.

Algorithm 11 Alarm Generation

```
Data: Output of Algorithm 9 and 10
Result: Alarms
if (STAGE-1-ATTACK-TRAFFIC = False and
  STAGE-2-ATTACK-TRAFFIC = False) then
    LOG as "No MC-MitM attack found"
end
if (STAGE-1-ATTACK-TRAFFIC = True and
  STAGE-2-ATTACK-TRAFFIC =True) then
    if (CONST-JAM = True and STAGE 2 ATTACK TRAFFIC =
      True) then
        Raise Alarm;
        LOG as "MC-MitM-BVC attack";
    end
    if (REACT-JAM = True and STAGE 2 ATTACK TRAFFIC =
      True then
        Raise Alarm;
        LOG as "MC-MitM-BVR attack";
    end
    if (CSA-ATTACK = True and STAGE 2 ATTACK TRAFFIC =
      True then
        Raise Alarm;
        LOG as "MC-MitM-IV attack";
    end
else
    if (STAGE-1-ATTACK-TRAFFIC = False and
      STAGE-2-ATTACK-TRAFFIC = True) then
        Raise Alarm;
        LOG as "MC-MitM-attack";
        LOG as "Attack variant unidentified";
    end
end
```

ACKNOWLEDGMENT

The authors wish to extend their special thanks to Mathy Vanhoef for providing source codes and helping in resolving some issues related to MC-MitM attacks.

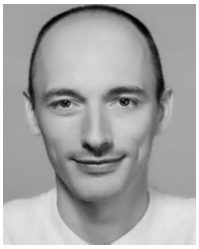
REFERENCES

[1] D. A. D. Zovi and S. A. Macaulay, "Attacking automatic wireless network selection," in *Proc. 6th Annu. IEEE Syst., Man Cybern. (SMC) Inf. Assurance Workshop*, Apr. 2005, pp. 365–372.
[2] B. Fajar. (2021). *Fluxion Kali Linux Tutorial*. [Online]. Available: https://linuxhint.com/fluxion-kali-linux-tutorial
[3] KaliTut. (2021). *Wifiphisher Evil Twin Attack*. [Online]. Available: https://kalitut.com/Wifiphisher-evil-twin-attack
[4] KaliTut. (2021). *WiFi Pumpkin Framework for Rogue WiFi Access Point Attack*. [Online]. Available: https://kalitut.com/wifi-pumpkin-framework-for-rogue-wi-fi
[5] Thecybersecurityman. (2018). *PenTest Edition: Creating an Evil Twin or Fake Access Point on Your Home Network Using Aircrack-NG and Dnsmasq*. [Online]. Available: https://thecybersecurityman.com/2018/08/11/pentest-edition-creating-an-evil-twin-or-fake-access-point-using-aircrack-ng-and-dnsmasq-part-1-setup
[6] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 256–265.
[7] M. Vanhoef and F. Piessens, "Release the kraken: New KRACKs in the 802.11 standard," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 299–314.
[8] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1313–1328.
[9] M. Vanhoef, "Fragment and forge: Breaking Wi-Fi through frame aggregation and fragmentation," in *Proc. 30th USENIX Secur. Symp. (USENIX Security)*, 2021, pp. 161–178.
[10] J. Freudenreich, J. Weidman, and J. Grossklags, "Responding to KRACK: Wi-Fi security awareness in private households," in *Human Aspects of Information Security and Assurance*. Cham, Switzerland: Springer, 2020, pp. 233–243.
[11] Security Focus. (2019). *WPA2 Key Reinstallation Multiple Security Weaknesses*. [Online]. Available: https://www.securityfocus.com/bid/101274
[12] M. Chi et al., "Multi-channel man-in-the-middle attack against communication-based train control systems: Attack implementation and impact," in *Lecture Notes in Electrical Engineering*. Singapore: Springer, 2020, pp. 129–139.
[13] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-channel man-in-the-middle attacks against protected Wi-Fi networks: A state of the art review," *Expert Syst. Appl.*, vol. 210, Dec. 2022, Art. no. 118401.
[14] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, "A novel approach for rogue access point detection on the client-side," in *Proc. 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Mar. 2012, pp. 684–687, doi: 10.1109/WAINA.2012.108.
[15] L. Wang and A. M. Wyglinski, "Detection of man-in-the-middle attacks using physical layer wireless security techniques," *Wireless Commun. Mobile Comput.*, vol. 16, no. 4, pp. 408–426, Mar. 2016.
[16] M. Vanhoef, P. Adhikari, and C. Pöpper, "Protecting Wi-Fi beacons from outsider forgeries," in *Proc. 13th ACM Conf. Security Privacy Wireless Mobile Netw.*, 2020, pp. 155–160.
[17] C. Louca, A. Peratikou, and S. Stavrou, "802.11 man-in-the-middle attack using channel switch announcement constantinos," in *Proc. 12th Int. Netw. Conf.* Cham, Switzerland: Springer, 2021, pp. 62–70.
[18] C. Louca, A. Peratikou, and S. Stavrou, "On the detection of channel switch announcement attack in 802.11 networks," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2021, pp. 281–285.
[19] S. Gong, H. Ochiai, and H. Esaki, "Scan-based self anomaly detection: Client-side mitigation of channel-based man-in-the-middle attacks against Wi-Fi," in *Proc. IEEE 44th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2020, pp. 1498–1503.
[20] S. Burke. (2018). *Wi-Fi Alliance Introduces Security Enhancements*. [Online]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements
[21] Philipp Ebbecke (Wi-Fi Alliance). (2020). *Protected Management Frames Enhance Wi-Fi Network Security*. [Online]. Available: https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security
[22] B. Bertka, "802.11w security? DoS attacks and vulnerability controls," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2012.
[23] M. Vanhoef. (2021). *FragAttacks: Clarifying Some Aspects*. Accessed: May 10, 2023. [Online]. Available: https://www.mathyvanhoef.com/2021/05/fragattacks-clarifying-some-aspects.html
[24] CWNP. (2009). *Wireless LAN Security and IEEE 802.11w*. [Online]. Available: https://www.cwnp.com/wireless-lan-security-and-ieee-802-11w
[25] MTROI. (2021). *Protected Management Frames (802.11w)*. [Online]. Available: https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w
[26] E. Chatzoglou, G. Kambourakis, and C. Kolias, "Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset," *IEEE Access*, vol. 9, pp. 34188–34205, 2021.
[27] M. Thankappan. (2023). *Signature-Based-WIDS-for-Detecting-MC-MitM-Attacks*. [Online]. Available: https://github.com/maneshthankappan/Signature-Based-WIDS-for-detecting-MC-MitM-attacks
[28] W. J. Tom Van Goethem, M. Vanhoef, and F. Piessens, "Request and conquer: Exposing cross-origin resource size," in *Proc. 25th USENIX Secur. Symp.*, 2016, pp. 447–462.
[29] M. Vanhoef and F. Piessens, "Predicting, decrypting, and abusing WPA2/802.11 group keys," in *Proc. 25th USENIX Secur. Symp. (USENIX Assoc.)*, 2016, pp. 673–688.
[30] L. F. Epia Realpe, O. J. S. Parra, and J. B. Velandia, "Use of KRACK attack to obtain sensitive information," in *Proc. Int. Conf. Mobile, Secure, Program. Netw.*, in Lecture Notes in Computer Science, vol. 11005, 2019, pp. 270–276.
[31] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *Proc. 2nd ACM Conf. Wireless Netw. Secur.*, Mar. 2009, pp. 79–85.
[32] J. Selvi, "Bypassing HTTP strict transport security," 2014. [Online]. Available: https://www.blackhat.com/docs/eu-14/materials/eu-14-Selvi-Bypassing-HTTPStrict-Transport-Security-wp.pdf
[33] C. Matte, J. P. Achara, and M. Cunche, "Device-to-identity linking attack using targeted Wi-Fi geolocation spoofing," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2015, pp. 1–6.
[34] M. Vanhoef, N. Bhandaru, T. Derham, I. Ouzieli, and F. Piessens, "Operating channel validation: Preventing multi-channel man-in-the-middle attacks against protected Wi-Fi networks," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2018, pp. 34–39.
[35] Wi-Fi Alliance. (2020). *SAE Public Key*. [Online]. Available: https://www.wi-fi.org/beacon/thomas-derham-nehru-bhandaru/wi-fi-certified-wpa3-december-2020-update-brings-new-0
[36] Huawei. (2020). *Wireless Access Controller Configuration Guide*. [Online]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100008282/b27702df/understanding-WLAN-security-policies
[37] U. Chatterjee, R. Sadhukhan, D. Mukhopadhyay, R. Subhra Chakraborty, D. Mahata, and M. M. Prabhu, "Stupify: A hardware countermeasure of KRACKs in WPA2 using physically unclonable functions," in *Proc. Companion Web Conf.*, Apr. 2020, pp. 217–221.
[38] A. Babaei and G. Schiele, "Physical unclonable functions in the Internet of Things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, Jul. 2019.
[39] T. Chin and K. Xiong, "KrackCover: A wireless security framework for covering KRACK attacks," in *Wireless Algorithms, Systems, and Applications*, vol. 10874. Cham, Switzerland: Springer, 2018.
[40] Y. Li, M. Serrano, T. Chin, K. Xiong, and J. Lin, "A software-defined networking-based detection and mitigation approach against Krack," in *Proc. 16th Int. Joint Conf. E-Business Telecommun.*, 2019, pp. 244–251.
[41] T. Naitik, L. Raiton, V. Pradnya, and S. Vamshi, "Mitigation of key reinstallation attack in WPA2 Wi-Fi networks by detection of nonce reuse," *Int. Res. J. Eng. Technol.*, vol. 5, no. 5, pp 1528–1531, 2018.
[42] Securingsam. (2017). *KRACK Detector*. [Online]. Available: https://github.com/securingsam/krackdetector.
[43] A. Agrawal, U. Chatterjee, and R. R. Maiti, "CheckShake: Passively detecting anomaly in Wi-Fi security handshake using gradient boosting based ensemble learning," *IEEE Trans. Dependable Secure Comput.*, pp. 1–13, 2023.
[44] E. Chatzoglou, G. Kambourakis, C. Smiliotopoulos, and C. Kolias, "Best of both worlds: Detecting application layer attacks through 802.11 and non-802.11 features," *Sensors*, vol. 22, no. 15, p. 5633, Jul. 2022.
[45] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," *Comput. Secur.*, vol. 92, May 2020, Art. no. 101752.

[46] A. Agrawal, U. Chatterjee, and R. R. Maiti, "KTRACKER: Passively tracking Krack using ML model," in *Proc. 12th ACM Conf. Data Appl. Secur. Privacy*, Apr. 2022, pp. 364–366.
[47] G. Abare and E. J. Garba, "A proposed model for enhanced security against key reinstallation attack on wireless networks," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 7, no. 3, pp. 21–27, 2019.
[48] R. R. Singh, J. Moreira, T. Chothia, and M. D. Ryan, "Modelling of 802.11 4-way handshake attacks and analysis of security properties," in *Security and Trust Management*. Cham, Switzerland: Springer, 2020, pp. 3–21.
[49] C. Cremers, B. Kiesl, and N. Medinger, "A formal analysis of IEEE 802.11's WPA2: Countering the kracks caused by cracking the counters," in *Proc. 29th USENIX Secur. Symp.*, 2020, pp. 1–17.
[50] SNORT. (2018). *Policy-Other WPA2 Key Reuse Tool Attempt*. [Online]. Available: https://www.snort.org/rule_docs/1-44640
[51] D. Schepers, M. Vanhoef, and A. Ranganathan, "A framework to test and fuzz Wi-Fi devices," in *Proc. 14th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2021, pp. 368–370.
[52] *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Standard 802.11ad-2012, 2012.
[53] *Broadband Radio Access Networks (BRAN); 5 GHz High Performance RLAN; Harmonized EN Covering the Essential Requirements of Article 3.2 of the R Directive, V1.8.1*, ETSI EN 301893, Mar. 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_en/301800_301899/301893/01.07.00_40/en_301893v010700o.pdf
[54] M. Vanhoef. (2015). *Advanced Wi-Fi Attacks Using Commodity Hardware*. [Online]. Available: https://github.com/vanhoefm/modwifi#constant-jamming
[55] L. Woody. (2018). *Mitm-Channel-Based-Package*. [Online]. Available: https://pypi.org/project/mitm-channel-based.
[56] O. Osanaiye, A. Alfa, and G. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, p. 1691, May 2018.
[57] O. Punal, I. Aktas, C. J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jul. 2014, pp. 1–10.
[58] *IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*, IEEE Standard 802.11ax, May 2021.
[59] Ubuntu. (2005). *Hostapd_Cli*. [Online]. Available: http://manpages.ubuntu.com/manpages/bionic/man1/hostapd_cli.1.html
[60] M. Thankappan. (2023). *MC-MitM Attack Signatures*. [Online]. Available: https://github.com/maneshthankappan/-MC-MitM-Attack-Dataset
[61] W. Zhou, A. Marshall, and Q. Gu, "A sliding window based management traffic clustering algorithm for 802.11 WLAN intrusion detection," in *Proc. Int. Fed. Inf. Process.*, 2006, p. 213.
[62] InscapeData. (2011). *Introduction To 802.11n Outdoor Wireless Networks*. [Online]. Available: https://www.inscapedata.com/pdf/80211n Technology.pdf
[63] J. Dugan. (2020). *What is IPerf/IPerf3*. [Online]. Available: https://iperf.fr
[64] V. Sathya, M. I. Rochman, and M. Ghosh, "Measurement-based coexistence studies of LAA & Wi-Fi deployments in Chicago," *IEEE Wireless Commun.*, vol. 28, no. 1, pp. 136–143, Feb. 2021.
[65] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A tutorial on IEEE 802.11ax high efficiency WLANs," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 197–216, 1st Quart., 2019.

MANESH THANKAPPAN (Member, IEEE) received the B.Tech. degree in information technology from Mahatma Gandhi University, Kerala, India, in 2006, and the M.Tech. degree in information security from the National Institute of Technology Karnataka, Surathkal, India, in 2011. He is currently pursuing the Ph.D. degree in networks and information technologies with Universitat Oberta de Catalunya (UOC), Spain, under the supervision of Dr. Helena Rifà-Pous and Dr. Carles Garrigues. From February 2006 to October 2012, he was with the Faculty of Computer Science and Engineering, Adi Shankra Institute of Engineering and Technology (ASIET), Cochin, India. From October 2012 to October 2018, he was with the Department of Computer Science, Prince Sattam Bin Abdulaziz University (PSAU), Saudi Arabia, as a Lecturer. He is a member of the K-riptography and Information Security for Open Networks (KISON) Research Group, UOC. His research interests include cybersecurity and network forensics, with a special focus on the security of wireless networks and the IoT systems.

HELENA RIFÀ-POUS (Member, IEEE) received the Ph.D. degree from Universitat Politècnica de Catalunya, in 2008. Since 2007, she has been an Associate Professor with the Department of Computer Science, Universitat Oberta de Catalunya (UOC). She is also a Coordinator of the M.Sc. Cybersecurity and Privacy Course, UOC, and conducts her research within the K-riptography and Information Security for Open Networks (KISON) Research Group, UOC. She has authored numerous articles in journals and conferences. Her research interests include security and privacy protocols, with a special interest in distributed and wireless networks, such as smart homes and the IoT. She participates as a reviewer for several journals and also serves as an editor.



CARLES GARRIGUES received the Ph.D. degree from Universitat Autònoma de Barcelona, in 2008, and the research accreditation degree from the Catalan Quality Agency (AQU), in 2018. He has two recognized research periods from AQU. He is currently an Associate Professor with the Department of Computer Science, Universitat Oberta de Catalunya. He also conducts his research with the K-riptography and Information Security for Open Networks (KISON) Research Group, UOC. In terms of scientific production, he has authored several publications indexed in the ISI JCR. He has published numerous articles at national and international congresses. His research interests include computer security and privacy, with a special focus on security in smart cities, smart homes, and the IoT environments in general. He participates as a reviewer for several scientific journals. He has also served on the program committee of several conferences.

5

A Distributed and Cooperative Wireless Intrusion Detection System (DC-SWIDS) Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-fi Networks

Eur. Phys. J. C manuscript No.
(will be inserted by the editor)

A Distributed and Cooperative Signature- Based Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks

Manesh Thankappan[a,1,2], **Helena Rifà-Pous** [b,1,3], **Carles Garrigues** [c,1,3]

[1]Estudis d'Informàtica Multimèdia i Telecomunicació, Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Barcelona, Spain
[2]Adi Shankara Institute of Engineering and Technology, Kalady, Kerala, India
[3]Center for Cybersecurity Research of Catalonia (CYBERCAT), Barcelona, Spain

Received: date / Accepted: date

Abstract A Multi-Channel Man-in-the-Middle (MC-MitM) attack is an advanced type of MitM attack, distinguished by its capability to alter encrypted wireless communications between the Access Point (AP) and clients within a Wi-Fi network. Notably, MC-MitM attacks can be executed against any Wi-Fi client, regardless of the method of authentication used with the AP. The Key Reinstallation Attacks (KRACK) from 2017-18 and the subsequent FragAttacks in 2021 are notable instances of MC-MitM attacks. These major security attacks have extensively impacted millions of Wi-Fi systems across the globe, especially affecting networks that include Internet of Things (IoT) devices. Current defense strategies are ineffective against these attacks due to various interoperability challenges and the necessary modifications to devices or protocols within the targeted Wi-Fi networks. This paper introduces a distributed and cooperative intrusion detection mechanism designed to improve the detection of various MC-MitM attacks across a broad area. Evaluation of the system demonstrates that this framework can effectively identify MC-MitM attacks with an average accuracy of 98%, when implemented across different locations within our experimental testbed.

Keywords Intrusion Detection · KRACK · MC-MitM attack · FragAttacks · Attack Signature · Distributed · Wi-Fi · WLAN

1 Introduction

Wi-Fi networks are prone to different kinds of Man-in-the-Middle (MitM) attacks where attackers intercept or manipulate information between user devices and the AP by spoofing the device characteristics. In conventional MitM attacks, perpetrators typically equip a device with dual wireless cards; one connects to a legitimate AP, while the other serves as a rogue AP by spoofing the legitimate one. For such rogue AP to function effectively, it must be configured with the same settings as the legitimate AP. Consequently, the attacker must acquire the Wi-Fi password of the original network to accurately duplicate these parameters in the rogue setup. Fluxion [1],and airbase-ng [2], etc. are some common tools to perform traditional rogue AP MitM attacks.

This paper focuses on the MC-MitM attack, one of the advanced MitM attacks introduced by Vanhoef et al [3]. In this type of MitM attack, the attacker deploys a PC or laptop equipped with two wireless adapters, each operating on a different channel, allowing them to modify the encrypted wireless data between the AP and the client without needing any legitimate Wi-Fi passphrases. Specifically, the MC-MitM attacker spoofs the legitimate AP on a different channel (other than the legitimate channel) and facilitates the relaying of all connection and data frames between these channels. This capability enables the attacker to communicate concurrently with both the client and the AP. Moreover, the method of transmitting frames across various channels is effective regardless of the client's authentication method with the network, rendering MC-MitM attacks feasible in both enterprise and personal Wi-Fi networks. Once the attacker achieves the MC-MitM position, they gain the ability to block, intercept, delay, modify, buffer, inject, and replay protected wireless frames transmitted between the client and the legitimate AP. These actions serve as the foundation for other MC-MitM enabled attacks. While MC-MitM attacks do not directly break any encryption, their primary purpose is to exploit on particular vulnerabilities (such as weaknesses in encryption or authentication processes) present in various Wi-Fi protocols (e.g., WPA,WPA2/3). This exploitation allows

[a]e-mail: mthankappan@uoc.edu
[b]e-mail: hrifa@uoc.edu
[c]e-mail: cgarrigueso@uoc.edu

attackers to access and potentially extract sensitive user data. To establish a MC-MitM position, attackers typically employ either specialized jamming techniques or CSA (channel switch announcement) to manipulate client devices into switching to channels under their control.In this paper, we categorize MC-MitM attacks that use jamming techniques as 'base variant' (MC-MitM-BV) and those that employ CSAs as an 'improved variant' (MC-MitM-IV). In [4] and [5], we explore the technical configurations and mechanisms, and assess the unique characteristics of various MC-MitM attack strategies.

The key reinstallation attack (KRACK) stands out as the most recognized MC-MitM base variant attacks. It targets a critical nonce reuse vulnerability during the 4-way handshake protocol in the IEEE 802.11 standards, as detailed in [6]. This vulnerability allows an attacker to easily decrypt Wi-Fi frames, especially from Linux and Android devices, as these platforms are prone to use an all-zero encryption key in response to key reinstallation attacks under WPA or WPA2 protocols. Notably, this vulnerability represents a significant issue affecting millions of Wi-Fi devices globally. It arises from an incorrect implementation of the standard and stands out as the first non-vendor specific problem of its kind.

FragAttacks [7] are the latest MC-MitM improved variant attacks. FragAttacks represent the latest non-vendor specific vulnerability that targets specific fragmentation and aggregation aspects of the 802.11 standards. This vulnerability enables attackers to transmit packets legitimately into protected wireless networks and to extract sensitive data from clients. In [4], we performed an in-depth analysis of multiple MC-MitM attacks as described in the existing literature, and explored their consequences on Wi-Fi systems.

In WLAN environments, conventional perimeter defense mechanisms like firewalls and VPNs are typically utilized to safeguard sensitive communications. Yet, these measures are ineffective against MC-MitM attacks, as these are link-layer attacks that occur beneath the level at which firewalls operate, which is within the higher layers of the network stack.

Beginning in 2018, the implementation of Protected Management Frames (PMF) has been mandated by the Wi-Fi Alliance to strengthen the security of management frames under the WPA2 and WPA3 protocols, aimed at mitigating risks from rogue AP and DoS attacks [8], [9]. PMF is designed to protect certain management frames, including action frames, disassociation, and deauthentication frames [10]. Despite these advancements, PMF falls short in providing comprehensive defense against MC-MitM attacks for several reasons: firstly, attackers executing MC-MitM do not typically rely on deauthentication packets to establish their position [11]; secondly, PMF lacks the capability to detect attacks through jamming [12]; and thirdly, MC-MitM attacks often employ beacons or probe responses, which are not covered by PMF's protective measures. Furthermore, in situations where the MC-MitM attacker possesses legitimate access to the network, they are capable of manipulating clients to connect to a malicious rogue AP using CSA action frames [13], [14]. This insider status significantly complicates the detection of such attacks in real-world scenarios.

In [4], we also extensively studied various challenges and technical feasibility associated with various MC-MitM defense mechanisms, highlighting the significant difficulties encountered in their implementation, particularly within Wi-Fi-based IoT environments such as smart homes. We discovered that, while not all commercial devices are equipped with patches, the management and maintenance of these devices demand technical expertise beyond what the average user possesses. Additionally, current defense strategies are inadequate for addressing these attacks due to various interoperability issues and the need for updates to devices or protocols

To this end, in our paper [15], we introduced a lightweight, centralized, and signature-based wireless intrusion detection system (SWIDS) framework. This plug-and-play system is designed for seamless integration into Wi-Fi or IoT environments, requiring no modifications to network settings or existing devices. It also provides continuous security against all variants of MC-MitM attacks. The core of our intrusion detection system framework is a set of specific attack signatures that identifies the behavior of MC-MitM attacks in terms of network patterns. Our centralized intrusion detection system framework effectively identifies MC-MitM attacks within a maximum time of 60 seconds, achieving a true positive rate (TPR) of 90% with short-distance detectors and 84% with long-distance detectors in Wi-Fi or IoT environments. We also demonstrated that our centralized intrusion detection system experiences frame loss that affects detection performance, especially with long-distance detectors.

In this paper, we improve our centralized SWIDS framework [15] and propose a novel framework for distributed intrusion detection by employing cooperative and autonomous detection systems to detect different MC-MitM attack variants. These autonomous detection systems make independent attack decisions in the places where they are deployed and communicate with each other by exchanging attack details through Message Queuing Telemetry Transport (MQTT) communication protocol. Our primary goal is to enhance the detection capabilities across a broad area, thereby mitigating frame loss via distributed intrusion detection systems. The results indicate that the proposed distributed framework efficiently detects MC-MitM attacks with an average accuracy above 95% when deployed at different locations within our experimental testbed that covers a wide area.

1.1 Contributions

This paper presents the following contributions:

1. Design of a distributed and cooperative signature-based wireless intrusion detection system (DC-SWIDS) framework tailored for border surveillance in any Wi-Fi network.
2. Development of an open-source prototype of the proposed DC-SWIDS framework using the python-scapy library [16].
3. Implementation of the DC-SWIDS framework on Raspberry Pi.
4. Empirical evaluation of the DC-SWIDS framework in an industry-relevant smart home environment using off-the-shelf IoT and Wi-Fi devices.

The structure of this paper is organized as follows: Section 2 outlines the related work; Section 3 introduces our proposed solution; Section 4 details the implementation of our proposed solution; Section 5 evaluates the efficacy of the proposed solution. Lastly, Section 6 offers conclusions and directions for future work.

2 Related Work

In this section, we examine the existing defense mechanisms for combating MC-MitM attacks. We categorize the mechanisms, which are designed to either detect or prevent such attacks, into two primary classifications: stage 1 and stage 2 defense mechanisms. The stage 1 mechanisms are designed to mitigate potential threats posed by attackers before they acquire the MC-MitM setup. This involves the identification of authentic attack vectors, encompassing factors like rogue channels, unauthorized devices, and falsified CSAs. Conversely, the second category of defense mechanisms is designed to protect against attacks facilitated by MC-MitM attacks, including scenarios like KRACK, FragAttacks, and cipher downgrades, etc., once the attacker has successfully established control over the MC-MitM setup.

2.1 Stage 1 Defense Mechanisms

SWIDS [15] is a framework designed to detect MC-MitM attacks. It identifies these attacks by analyzing specific patterns or behaviors they exhibit. This system is user-friendly, lightweight, and compatible with any Wi-Fi-based IoT setup without requiring changes to existing devices or network configurations. Through testing in real scenarios, the system's effectiveness has been confirmed for both personal and enterprise Wi-Fi networks.

In [17], the authors introduced the Operating Channel Validation (OCV) method, to detect and prevent MC-MitM attacks by cryptographically validating the communication channel between the client and the AP. This method suggests extending the 802.11w standards (PMF standards) by including an (OCI) element. During the 4-way handshake messages, the OCI element within handshake frames undergoes authentication to ensure alignment of communication channels between the client and the AP. Although OCV has been integrated into IEEE standards, it is not a compulsory feature in WPA/2 standards and has not widely been implemented or accepted by device manufacturers. The effectiveness of OCV is limited to devices capable of Protected Management Frames (PMF), and even then, only if the PMF standards themselves are adapted, which is a significant challenge due to the complexity of setting or updating PMF across all devices. Furthermore, within a network enabled by OCV, insider attackers are still able to mimic CSAs and manipulate or replay previously captured CSAs to redirect clients to their channels, facilitating various MitM attacks.

In [18], an alternative approach was proposed to counteract attacks exploiting unprotected beacons, aiming to detect and prevent rogue AP, including MC-MitM attacks. The authors introduced an additional information element (IE) into each beacon, permitting clients to cryptographically validate beacon integrity during AP connections. However, similar to their previous work [17], the practical implementation of the beacon protection mechanism faces challenges predominantly due to the reliance on PMF. This can lead to interoperability concerns when employing devices that only support WPA or WPA2. Furthermore, it is important to mention that the proposed mechanism does not address the possibility of insider MC-MitM attacks[19]. Although the above mechanisms outlined in [17] and [18] can detect the presence of MC-MitM attacks,they are unable to accurately determine the specific variant of the attack being employed.

The WPA3-2020 updates introduced an additional feature, Simultaneous Authentication of Equals Public Key (SAE PK) [20], as part of the WLAN connection process to prevent MitM attacks in general. SAE-PK utilizes ECC (Elliptic Curve Cryptography) to uniquely identify APs during connection establishment. This feature also offers defense against insider attackers aiming to establish rogue APs and conduct MitM attacks through the use of the digital signature of the public key of the AP.

However, the detection of rogue APs through SAE-PK is primarily limited to the authentication phase or the initial client-AP connection. Conversely, MC-MitM attackers often position themselves between an already connected client and the AP, a scenario not entirely addressed by SAE-PK. Furthermore, it is important to note that [21] highlights that WPA3 clients utilize open authentication instead of SAE authentication during reconnection to an established network, potentially allowing MC-MitM attackers to bypass SAE security measures.

The authors in [22] introduced a method for detecting and preventing attacks using Physically Unclonable Func-

tions (PUF) to combat rogue AP used in MC-MitM attacks. This approach generates a unique key based on the AP's PUF signature to facilitate authentication between the AP and client devices. Nonetheless, the adoption of this PUF-based method necessitates intricate hardware alterations across all involved wireless devices. Furthermore, this technique remains susceptible to specific MitM attack variants [23].

In [24], the authors introduced a defense mechanism for wireless clients to identify the presence of rogue while launching MC-MitM-BVR attacks. This involved developing a modification for wpa-supplicant (wireless client software application), which verifies the uniqueness of paired identifiers such as BSSID and SSID during client-AP communication. However, this method faces challenges if an MC-MitM attacker continuously jams the legitimate AP's channel, preventing the client from collecting the necessary beacon data for verification. Moreover, relying solely on the distinctiveness of SSID and BSSID pairs is insufficient in scenarios where these identifiers are duplicated, particularly in environments where APs facilitate dual-band connections. Additionally, SSAD is only capable of detecting base variant (MC-MitM-BV) attacks and not the improved variant (MC-MitM-IV) attacks, as it fails to identify counterfeit CSAs.

2.2 Stage 2 Defense Mechanisms

Many stage 2 defense strategies are designed specifically to detect or counteract MC-MitM-enabled KRACK attacks due to their significant effects on Wi-Fi system security. Certain mechanisms, including those outlined in [25], [26], [27], and [28] utilize network analysis techniques to identify retransmissions of Message 3 in the 4-way handshake process specific to KRACK attacks. Nevertheless, the 802.11 standards consider APs re-transmitting Message 3 under specific circumstances, such as network congestion or reaching retransmission limits. Blocking re-transmissions of handshake messages can lead to frequent failures or increased false positives.

In [29], a recent study introduced anomaly detection, utilizing supervised machine learning models to identify handshake messages across various channels, particularly focusing on detecting KRACK behavior. Although effective in KRACK detection, their focus remains limited to this specific type of MC-MitM enabled attack and is not evaluated in any real world settings. This lack of practical evaluation limits its feasibility in defending against real time attacks. Similar works, such as [30],[31],and [32] also have not undergone real-network evaluations, relying the use of AWID3 public dataset [33]. In our paper [15], we showed the enhanced efficiency of our SWIDS framework in identifying KRACK attacks from AWID3 datasets, outperforming similar defense mechanisms.

In contrast, mechanisms discussed in [34], [35], and [36] introduce cryptographic verification methods during the 4-way handshake exchanges to combat nonce reuse vulnerabilities targeted by KRACK. These approaches additionally tackle cipher downgrade attacks on APs. However, their deployment requires modifications to Wi-Fi standards and has not been evaluated in actual attack environments.

Regarding FragAttacks, dedicated defense mechanisms are currently absent. Instead, a testing framework [37] has been established to detect fragmentation and aggregation vulnerabilities in Wi-Fi devices.

In [38], Snort rules designed to detect network packets that carry distinct markers associated with KRACK attack scripts. However, modified versions of KRACK attacks may not be detected by these rules. Furthermore, the markers identified could also be present in legitimate WLAN packets or in scripts from other attacks crafted using Scapy. Consequently, exclusive reliance on predefined Snort rules could lead to ineffective detection or false positives.

2.3 Significant Research Challenges

Overall, the defense mechanisms currently in place fail to provide a holistic solution capable of effectively detecting all types of MC-MitM attacks. Furthermore, we underscore the design shortcomings of current standards, pointing out the absence of research that adequately protects PMF clients from MC-MitM attacks, which can elude PMF protection through various methods. This gap represents a significant ongoing research challenge, particularly with new WPA2 and WPA3 devices that now require PMF. MC-MitM attacks are particularly critical when perpetrated by insiders or authorized users, such as through fragmentation cache attacks [7], potentially leading to the compromise of private communications within homes or offices. Existing defense strategies are insufficient to address these complex scenarios effectively.

From an operational standpoint, existing defense strategies, with the exception of SWIDS [15] as mentioned earlier, demand firmware updates or the implementation of specific software/hardware solutions across wireless devices. Consequently, their efficiency is contingent upon the universal compatibility of devices within a WLAN, a criterion not universally met by IoT devices or all Wi-Fi clients. This requirement often imposes considerable technical challenges on end-users in terms of device and network setup and maintenance. Furthermore, the majority of these defense solutions lacks empirical validation in real-world Wi-Fi or IoT scenarios, thereby constraining their practical utility. Additionally, existing defense mechanisms fail to offer backward compatibility with older or deprecated devices. This scenario underscores the pressing need for the development of more useful and user-friendly defense strategies that can cater to

the diverse landscape of Wi-Fi enabled devices and their security needs.

2.4 SWIDS: A Signature-Based Wireless Intrusion Detection System Framework for MC-MitM attacks

Considering diverse challenges and technical infeasibility concerns, in [15] we designed the first centralized, lightweight and SWIDS framework, specifically tailored for the demands of Wi-Fi or IoT-driven smart environments. The SWIDS framework we have developed possesses the capability to detect a variety of MC-MitM attacks, which constitute the underlying basis for more recognized attacks, including but not limited to KRACK [6] and FragAttacks [7]. Instead of relying on machine learning, the framework adopts a threshold based detection approach that meticulously examines wireless network frames to rapidly identify attack signatures or suspicious behaviors in a WLAN during a probe interval duration (specific observation period for observing wireless frames). In our previous paper [15], we elaborate on the formulation of MC-MitM attack signatures in Section IV, the design of the probe interval, and the intricacies of our detection methodology, along with its integration into the SWIDS framework, as discussed in Section V. Additionally, Appendix A of the aforementioned paper provides an exposition of the network analysis algorithms that play a crucial role in the identification of a spectrum of MC-MitM attack signatures. The detection methodology is based on both theoretical and empirical analysis of Wi-Fi protocol operation (benign traffic) and the attack traffic. Our SWIDS framework functions in real-time, analyzing Wi-Fi frames and immediately identifying potential attacks by detecting malicious frames. This plug-and-play system effortlessly integrates into existing Wi-Fi or IoT setups without requiring modifications to current network configurations or devices. It reliably protects against all types of MC-MitM attacks. In real-world Wi-Fi or IoT environments, our short-distance detectors achieve an average TPR of 90%. Meanwhile, our long-distance detectors maintain an average TPR of 84% in identifying different MC-MitM attacks.

2.5 Limitations of centralized SWIDS framework

The SWIDS framework captures wireless frames in real time, but suffers from frame losses that impair the detection accuracy of MC-MitM attacks. These losses are particularly pronounced in detectors located more than 10 meters away from the attacker, and can be attributed to various factors including network conditions, the time taken to parse and process frames, and the processing capabilities of the Wi-Fi card. As a result, the centralized SWIDS system may incorrectly classify some attacks as benign or fail to accurately identify attacks, leading to a decrease in detection performance.

In our experiments evaluating detection capabilities with contemporary Wi-Fi routers, such as 802.11ac and 802.11ax, we concentrated on the impact of varying channel widths and the functions of primary and secondary channels. We discovered that the primary cause of reduced performance was frame loss, which could be attributed either to the distance between the detector and the attacker or to delays in processing frames within the SWIDS framework. Additionally, network conditions and environmental elements like traffic density, network overhead, and building materials, etc., also impacted the wireless signal range and throughput, thereby affecting detection efficiency.

Furthermore, the entire system's reliability and availability are at risk if the centralized detection system fails for any reason. Another limitation is that the framework can monitor only one Wi-Fi network or AP at a time, lacking the ability to simultaneously monitor multiple APs or channels, including both 2.4 GHz and 5 GHz frequencies. These challenges have led us to propose a distributed architecture for detecting MC-MitM attacks, aiming to overcome these limitations and improve detection accuracy and system reliability.

3 Proposed Solution:- A Distributed And Cooperative Signature Based Wireless Intrusion Detection System Framework For MC-MitM Attacks

3.1 System Architecture of the DC-SWIDS Framework

The DC-SWIDS framework is designed as a network system incorporating distributed Autonomous Detection System (ADS) nodes, each functioning as an evolution of our previously centralized SWIDS framework. Fig. 1 illustrates an example of the DC-SWIDS framework featuring four ADS nodes.

Various ADS nodes in the DC-SWIDS framework are interconnected through the existing WLAN and communicate with each other using the Message Queuing Telemetry Transport (MQTT) protocol. This setup enables each ADS node to act as a MQTT client and incorporates a cooperative unit designed for interconnection with other ADS nodes through a cloud-based MQTT broker. The primary function of each ADS node is to autonomously monitor wireless traffic within their designated areas, identifying the presence of MC-MitM attacks and also exchanging statuses of stage 1 and 2 attack traffic via the MQTT broker with other ADS nodes. Furthermore, each ADS node is capable of monitoring either a single AP or different APs simultaneously.

To enforce the integrity and confidentiality of exchanged messages from eavesdroppers or attackers, we use a TLS (Transport Layer Security) enabled MQTT broker. Specifically, we employ MQTT with authentication, powered by

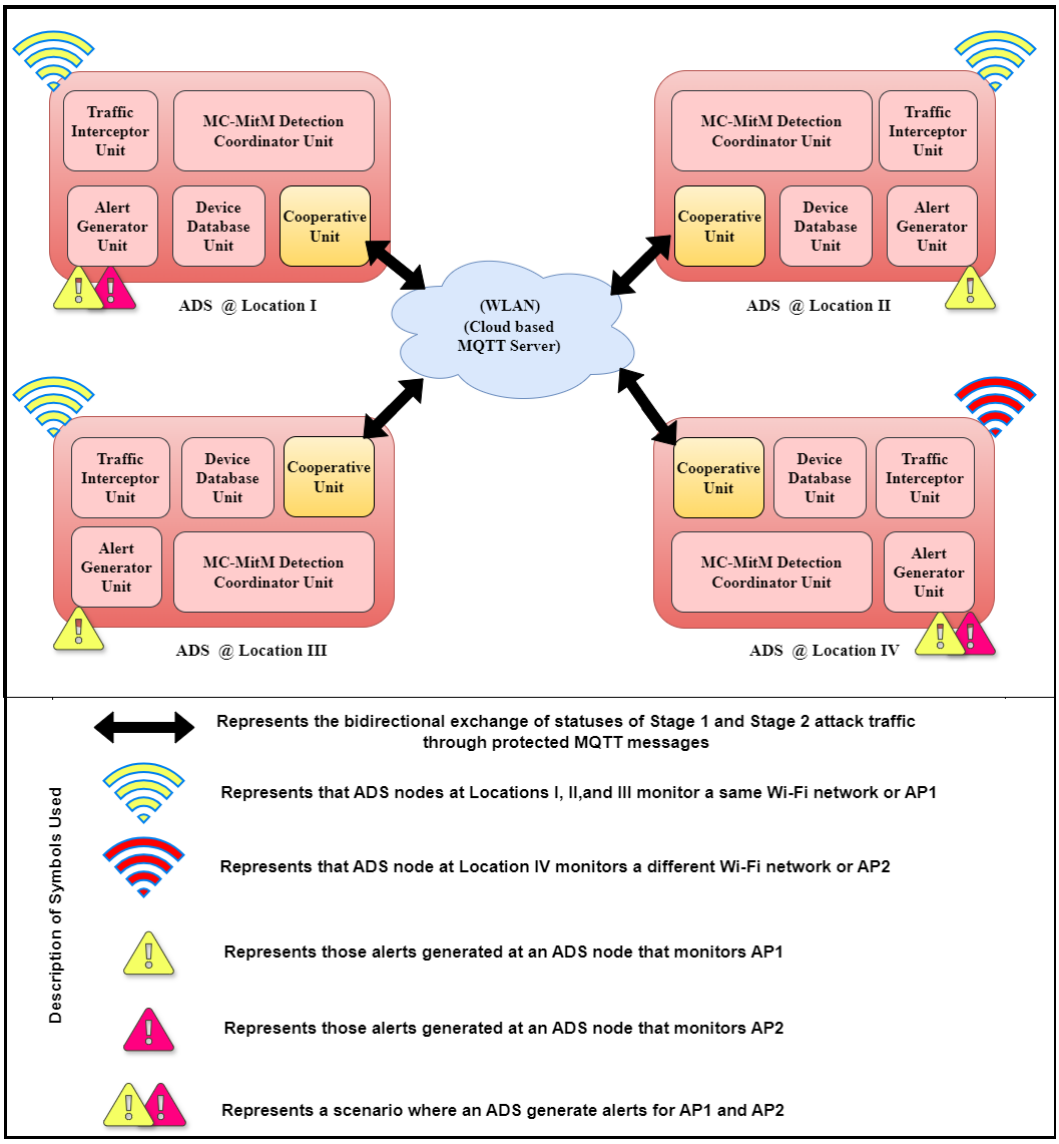


Fig. 1 A Model of DC-SWIDS Framework

TLS. This approach establishes a secure tunnel between ADS nodes (acting as MQTT clients) and the MQTT broker, safeguarding the confidentiality of data as it travels through the network. The broker also provides authentication and access control, so that only authorized ADS nodes can connect and authenticate to the broker. This secured configuration prevents potential attackers from setting up unauthorized ADS nodes.

In the event that an MC-MitM attack disrupts (for example, through jamming) one or more ADS nodes, the neighboring nodes are capable of promptly detecting such disruptions (see Section IV.B.1 of our SWIDS paper [15]). They can then disseminate the jamming attack data to other interconnected ADS nodes through the cooperative unit. This capability underscores the resilience of the system against attempts to evade or delay detection through interference with its components.

Specifically, within a given probe interval duration, every ADS node broadcasts or transmits the observed local statuses of stage 1 and 2 attack traffic, while also receiving those statuses from other ADS nodes deployed at various locations through the cooperative unit. In the event of any ADS node failing to detect MC-MitM attacks, other ADS nodes can continue to detect attacks cooperatively. For example, if an ADS node could not identify a particular attack status, possibly due to frame loss or other reasons, the cooperative unit can compensate for the missed detections by receiving attack statuses from other deployed ADS nodes. Consequently, alerts for MC-MitM attacks are generated by individual ADS nodes when such attacks are detected. Moreover, the exchange of attack data via cooperative communi-

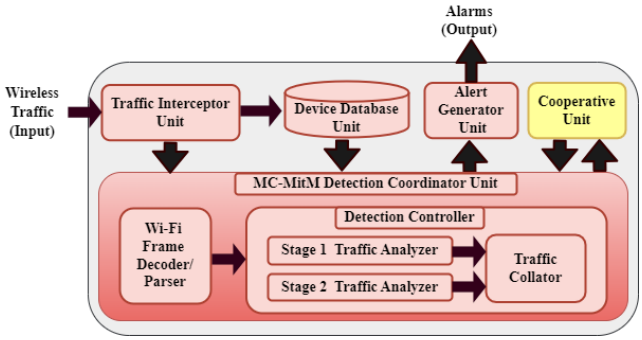


Fig. 2 High level system architecture of an ADS node in the DC-SWIDS framework

cation enables other ADS nodes to issue alerts at the same or subsequent probe intervals.

It is also important to mention that not all ADS nodes need to issue alerts at the same time; the generation of alerts depends on the availability of local attack data or data provided by other ADS during a probe interval. This collaborative approach also overcomes the problem of having a single detection node, which becomes a single point of failure in the WLAN.

In the next section, we illustrate the high-level system architecture and workflow of an ADS in the DC-SWIDS framework.

3.2 System Architecture of an ADS node in the DC-SWIDS framework

Fig. 2 illustrates the high-level system architecture and workflow of an ADS in the DC-SWIDS framework, which is structured around five primary units: the traffic interceptor, device database unit, MC-MitM detection coordinator unit, the alert generator unit, and cooperative unit. In the following sections, we provide an explanation of each unit within the framework.

3.2.1 Traffic interceptor unit

As shown in Fig.2, a traffic interceptor unit passively monitors the wireless traffic of a specific AP and connected clients in a deployed location. It primerly filters required beacons, probe responses, connection establishment frames, etc., based on the AP's MAC address. These filtered frames are then forwarded to both the device database and the MC-MitM detection coordinator units for more in-depth analysis.

3.2.2 Device database unit

The device database unit collects MAC addresses of clients connected to a specific AP in the WLAN before attack detection. This data is crucial as it aids the MC-MitM detection coordinator unit in identifying potential attack signatures and effectively detecting attacks. Additionally, whenever a new Wi-Fi client connects to the target access point, this unit automatically compiles information about all such newly connected devices and appropriately updates the database.

3.2.3 MC-MitM detection coordinator unit

The MC-MitM detection unit mainly identifies attack signatures of MC-MitM attacks from the filtered wireless traffic in the vicinity of an ADS. The unit has two key modules.

Wi-Fi frame decoder: This component processes and decodes each wireless frame, pulling essential data from the MAC layer header such as type, subtype, BSSID, ESSID, and channel used, among others. After extracting this information, the parsed frames are sent to the detection controller.

Detection controller: This module implements the detection methodology and network traffic analysis algorithms to identify the specific attack traffic associated with MC-MitM attack variants. It maintains three sub-modules. The Stage 1 and Stage 2 traffic analyzer sub-modules, which track and record the number of network frames corresponding to the Stage 1 and Stage 2 attack signatures over a given probe interval. After the completion of a probe interval, the traffic collator sub-module evaluates the data on Stage 1 and Stage 2 attack traffic against preset threshold values (see Table II of our SWIDS [15]). It then forwards the statuses of attack signatures identified locally to the cooperative unit and also verifies the statuses of the remote attack traffic received by the cooperative unit. Based on these attack statuses, which are found locally and received remotely, the traffic collator sub-module in a single ADS node decides whether the MC-MitM attack is occurring in any part of a particular WLAN, traces its variant, and forwards the attack details to the alert generator unit.

3.2.4 Cooperative unit

The cooperative unit plays a vital role in the DC-SWIDS framework. Its primary function is to collaborate with multiple ADSs using the MQTT protocol. This unit incorporates an MQTT client to support the communication process, specifically facilitating the exchange of information regarding various stages of MC-MitM attack traffic between ADS nodes through a centralized MQTT broker. The MQTT broker organizes the information on attack traffic into topics, with each ADS node both subscribing to and publishing on these topics. Subscription allows the cooperative unit to receive updates on attack statuses from other ADS nodes, while publishing permits the dissemination of attack information to the network, ensuring a comprehensive and collaborative detection and response system. This collaboration enables the accurate detection of different MC-MitM attacks.

3.2.5 Alert generator unit

This unit generates alerts for MC-MitM attacks based on notifications from the MC-MitM detection controller within an ADS node, as shown in Fig.2. Additionally, the alert generator unit records these alerts along with the MAC addresses of the victims and the specific time and date of each attack.

3.3 Capacity planning

One of the key objectives within the DC-SWIDS framework is determining the minimum number of ADS units necessary to achieve a true positive rate (TPR) exceeding 95%, along with planning their distribution. This parameter holds significant importance in ensuring effective surveillance and defense mechanisms while avoiding unnecessary deployment of detectors, which could result in over saturation. To do this, we first determine the maximum distance between a deployed ADS node and a potential attacker while ensuring a TPR of 95% or higher. Subsequently, based on this maximum distance, we define a circular surveillance area with the radius equal to the established maximum distance. In section 5, we present the evaluation based on this capacity planning, and in section 5.2 we show the experiments carried out to determine the maximum distance between ADS nodes. This approach offers a cost-effective solution, particularly in large-scale or complex environments. The task of determining the optimal number of ADS units for a given environment is comparable to placing base stations in cellular networks and poses a similar challenge. Considerable research, spanning academic and industrial sectors, has been devoted to this endeavor, as evidenced by existing literature [39].

4 Proposed Solution:- System Implementation and Setup

In this section, we provide an overview of how our DC-SWIDS framework is implemented, the key graphical user interfaces (GUIs) developed during the prototyping phase and detail the setup process within a real world IoT environment.

4.1 Framework implementation

We develop our DC-SWIDS framework using Python. More specifically, an ADS of our DC-SWIDS framework, as depicted in Fig.2, is composed of four distinct units developed using Python-Scapy libraries, which are utilized for network packet processing. The ADS's traffic interception unit is implemented with the help of two wireless interfaces, specifically the TL-WN722N for the 2.4 GHz band and Wi-Fi Nation for the 5 GHz band, selected for their affordability and

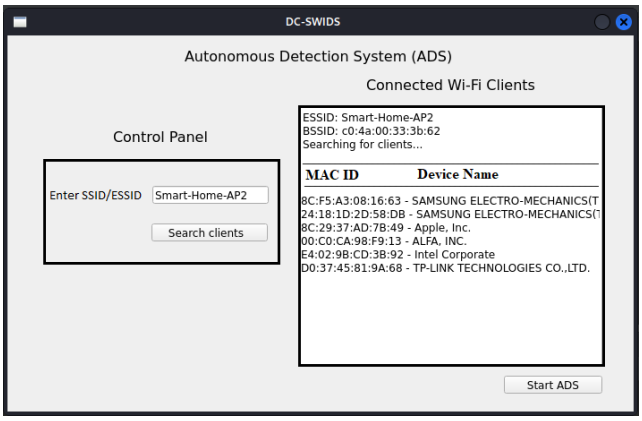


Fig. 3 Screenshot of the front panel of an ADS in DC-SWIDS framework

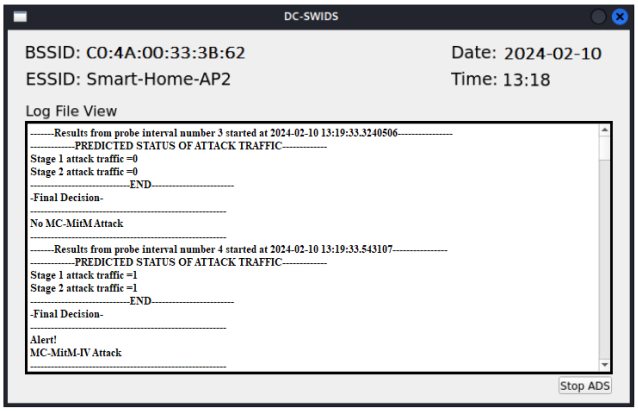


Fig. 4 Screenshot of the log file view panel of an ADS node in DC-SWIDS framework

compatibility with monitor mode across various Linux distributions. Moreover, we have integrated a text based logging mechanism to efficiently record all alerts triggered within our system. Additionally, to develop the cooperative unit, we employ a pre-configured MQTT account on a cloud-supported platform. In our tests, we employed the EMQX broker: a free, rapid, and cloud-based MQTT service. Importantly, each ADS node must be connected to the existing WLAN to maintain internet access. Finally, the hardware used to build the ADS node is a Raspberry Pi 4 and the script used in an ADS node is made available in [16]

4.2 System setup in real-world environment

In our proposed system, we have developed a graphical user interface (GUI) as a proof of concept for activating an ADS node, illustrated in Fig.3. This GUI simplifies the initial setup process, requiring users to only input the SSID (Wi-Fi network name) of the AP or Wi-Fi network targeted for surveillance. By activating the "search clients" function, the ADS

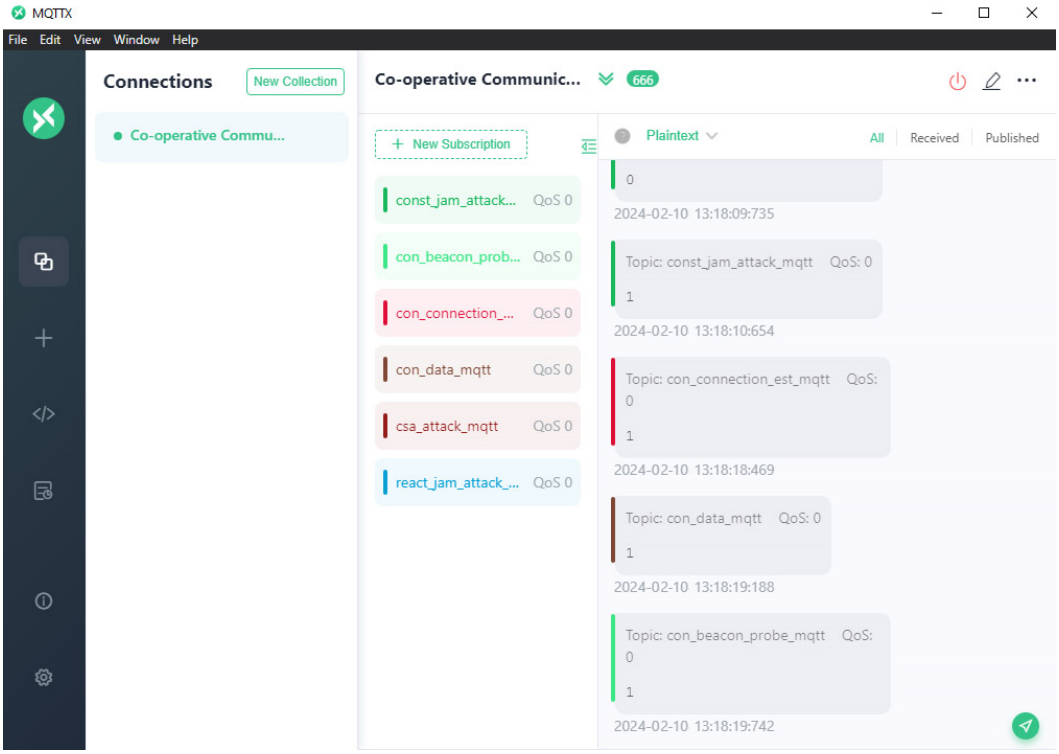


Fig. 5 Screenshot of a sample cooperative communication (exchange of statues of attack traffic) for the detection of MC-MitM attacks

node efficiently identifies and catalogs all devices connected to the AP, detailing their MAC IDs and additional device information. Upon enumerating the connected devices, the ADS node is equipped to commence surveillance for MC-MitM attacks and initiate communication with similarly deployed ADS nodes using pre-configured MQTT credentials. Additionally, the system is designed to notify users of detected attacks via an audible alarm. Fig.4 displays the GUI tailored for log file review within the ADS framework, and Fig.5 showcases an instance of cooperative communication (the exchange of attack traffic data) during the network monitoring process, as captured from the MQTT broker. Finally, Fig.6 and 7 outlines the deployment of ADS nodes on a Raspberry Pi, accommodating various Wi-Fi frequencies. Two wireless adapters are employed to simultaneously track both the legitimate and rogue channels.

It is important to emphasize that the process of activating an ADS node has been simplified to mirror the ease of connecting to a Wi-Fi network, a task with which most users are already familiar. Following the completion of the initial activation, managing the DC-SWIDS framework is intended to be intuitive, necessitating minimal user effort. In future developments, we aim to evolve the DC-SWIDS framework into an installable plugin application, facilitating seamless integration with smart home ecosystems such as Home Assistant [40] or OpenHAB [41].

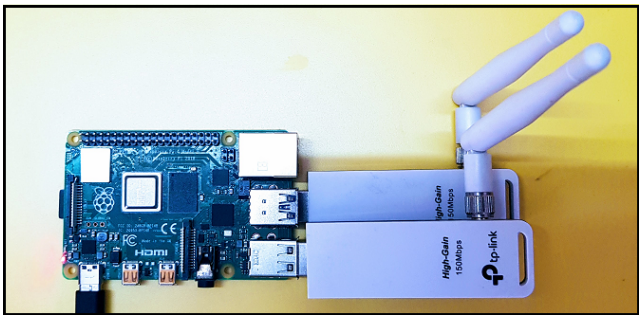


Fig. 6 An ADS node in the DC-SWIDS framework with support for 2.4 GHz

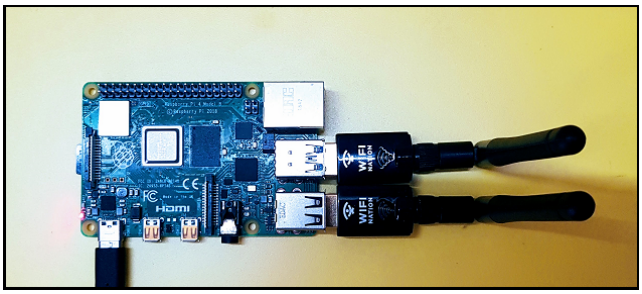


Fig. 7 An ADS node in the DC-SWIDS framework with support for 5 GHz

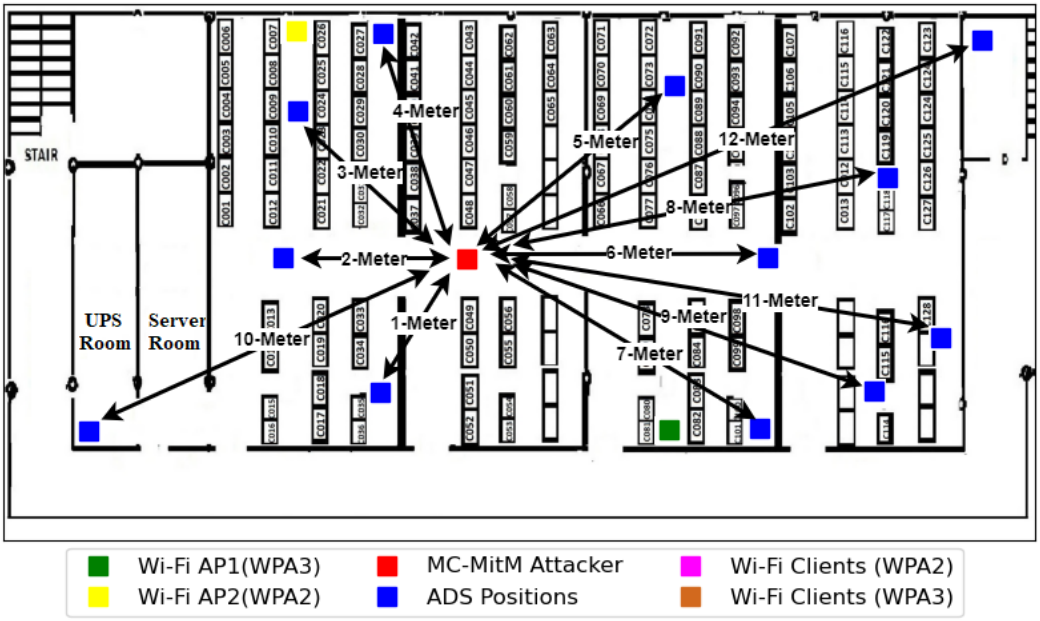


Fig. 8 Experimental testbed (distances are representative)

5 Evaluation

In this section, we evaluate the proposed DC-SWIDS framework for detecting MC-MitM attacks in a representative set of scenarios, focusing primarily on personal networks, but applicable to enterprise networks as well.

5.1 Experimental Testbed

The experimental phase was conducted within the central computing facility of our University, spanning an area of 500 square meters. Fig.8 depicts our experimental setup, showing the positions of test devices. Our objective was to determine the maximum distance between an attacker and an ADS node that shows a TPR of over 95%. We employed a total of 14 devices for this experiment, comprising 2APs, 9 client devices, 2 attacker devices, and an ADS node. Comprehensive device details are elaborated in Table 1. We established a mixed-mode Wi-Fi environment, integrating both WPA2 and WPA3 protocols, to support the connectivity of various devices. Specifically, 5 WPA2-compatible clients connected to AP1, and 4 WPA3-compatible clients connected to AP2. For executing MC-MitM attacks, individually, two laptops were employed: one for initiating MC-MitM-IV attacks and the other for conducting either MC-MitM-BVC or MC-MitM-BVR attacks.

To conduct experiments, we placed an ADS node of the DC-SWIDS framework, one at a time at varying distances from a fixed attacker location, starting from 1 meter and extending up to 12 meters, with each increment being 1 meter, as illustrated in Fig. 8. We established a distance limit of up

Table 1 Equipment utilized in the experimental setup

Device	Role	Wi-Fi Standard
TP-LINK Wireless Router (802.11 N), with a maximum speed of 144 Mbps, operates on Channel 1 (2.4 GHz) and has a transmission power ranging from 25 to 30 dBm.	Wi-Fi AP1	WPA2-PSK
Samsung S8	AP1 Client	WPA2
Panasonic LED Bulb	AP1 Client	WPA2
Zebronics Plug-SP110	AP1 Client	WPA2
Smart TV	AP1 Client	WPA2
D-Link Wireless AX 1500 (802.11 B/G/N) Wi-Fi 6 Router, capable of speeds up to 1200 Mbps, operates on Channel 36 (5 GHz) with a transmission power of 14 dBm	Wi-Fi AP2	WPA3-SAE
Samsung S23	AP2 Client	WPA2
iPad Mini	AP2 Client	WPA3
Samsung S22	AP2 Client	WPA3
Dell Inspiron 15	AP2 Client	WPA3
Lenovo-Thinkpad	MC-MitM-IV Attacker	WPA2/3
Toshiba Portege R500	MC-MitM-BV Attacker	WPA2/3
Raspberry Pi 4 equipped with TP-Link TL-WN722N and Wi-Fi Nation high-gain Wi-Fi adapters.	ADS node of DC-SWIDS Framework	any

Table 2 Summary of evaluation metrics

Metric	Description	Method
TPR (True positive rate)	Ratio of accurate positives compared to the overall actual positives	(TP) / (TP + FN)
TNR (True negative rate)	Ratio of accurate negatives in relation to the total number of actual negatives.	TN / (FP + TN)
F1-score	Harmonic mean of precision and TPR	2TP / (2TP + FP + FN)

to 12 meters, as evidenced in our previous work [15], demonstrating that distances beyond this threshold could lead to significant frame loss, thereby impacting detection capabilities. Specifically, we carried out 75 tests for each distance, with 25 tests dedicated to each of the three MC-MitM attack variants, conducted at the aforementioned four distances. The findings from this initial series of experiments are detailed in Section 5.3.

5.2 Evaluation Methodology

The performance of our DC-SWIDS framework is evaluated using the metrics detailed in Table 2. Within this evaluation, each outcome from our framework is categorized as follows: TP (true positive) occurs when an alarm is correctly triggered during an attack; TN (true negative) when no alarm is triggered and there is no attack; FP (false positive) when an alarm is erroneously triggered without an attack; and FN (false negative) when an attack occurs but no alarm is generated.

5.3 Results and discussion of experiments to find out maximum distance with best (TPR above 95%) detection performance

Fig. 9 provides detection performance achieved by an ADS of our framework at different distances from the attacker location.

From Fig.9, we can observe that a single ADS node is capable of identifying various MC-MitM attack variants with a minimal TPR of 95% or higher, starting from a distance of 7 meters away from the attacker. Consequently, our experiments have led to the conclusion that situating an ADS node within a 7-meter radius effectively reduces frame loss, encompassing a surveillance area of roughly 150 square meters. Furthermore, it is crucial for users to maintain a maximum separation of 12 meters between the attacker and an ADS node to ensure a reasonable detection performance as mentioned in the previous section. In the following section, we evaluate our proposed DC-SWIDS framework, incorporating the necessary number of ADS nodes within a comprehensive and extensive Wi-Fi or IoT environment.

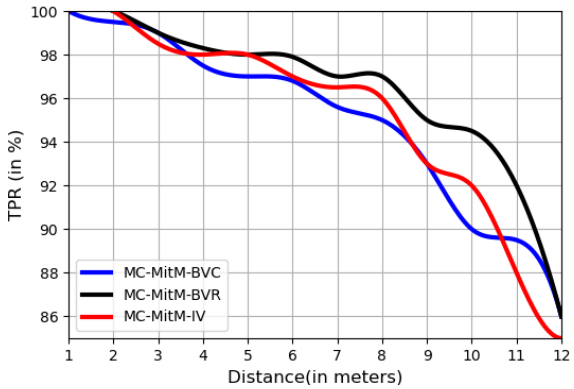


Fig. 9 Detection performance achieved with an ADS node when placed at different distances from the attacker.

5.4 Experimental testbed to analyze performance of DC-SWIDS framework in a Wi-Fi or IoT environment.

As shown in Fig.10, we have used our central computing facility at the University, which covers an area of 500 square meters, for the evaluation of our DC-SWIDS framework. Based on the optimal distance identified in the previous section, it is ascertained that 3 ADS nodes, spaced 7 meters apart, are required to achieve comprehensive coverage within the specified experimental testbed.

Our primary focus during testing lies in scrutinizing the detection performance of our DC-SWIDS framework across diverse attack scenarios, encompassing both fixed and moving attacker positions. Testing against both fixed and moving attacker positions is crucial because it mirrors the dynamic nature of MC-MitM attacks, where attackers may either persistently target a specific Wi-Fi client or shift their focus to evade detection. Such versatility underscores the DC-SWIDS framework's ability to provide robust security across a spectrum of attack methodologies, enhancing its reliability and effectiveness in safeguarding Wi-Fi networks against malicious MC-MitM attacks.

To ensure consistency, we maintained the identical device configuration detailed in Table 1. Regarding tests, for each attacker position, we conducted a series of 75 detection tests, comprising 25 detection tests for each of the three MC-MitM attack variants. These attacks were launched at five different positions but at different times, which are shown in Fig. 10. This resulted in a total of 375 detection tests.

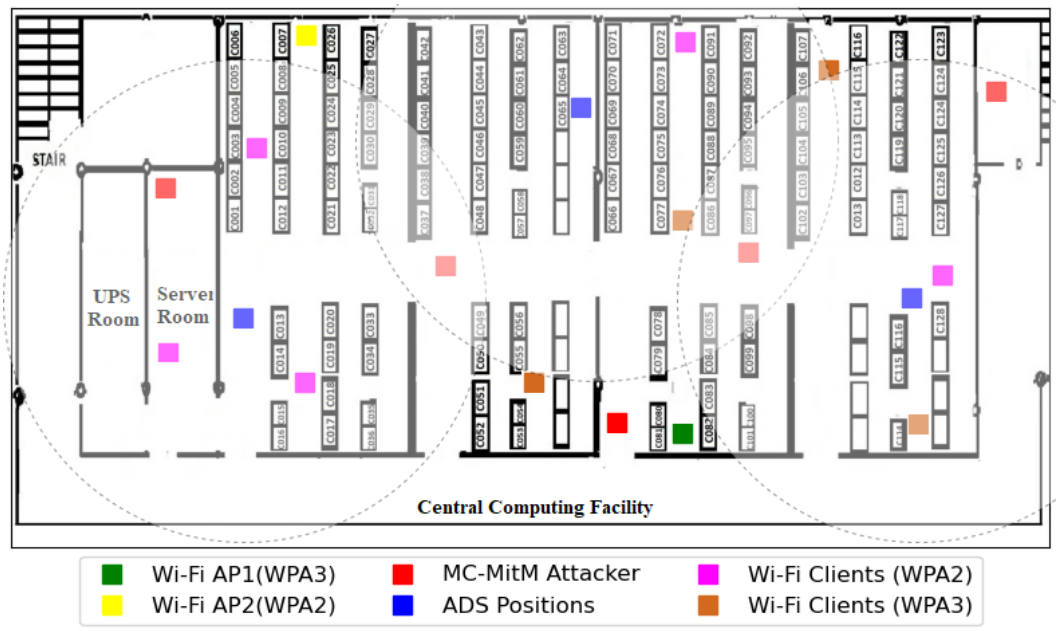


Fig. 10 Experimental testbed for implementation of DC-SWIDS framework (Devices used are same as in Table 1)

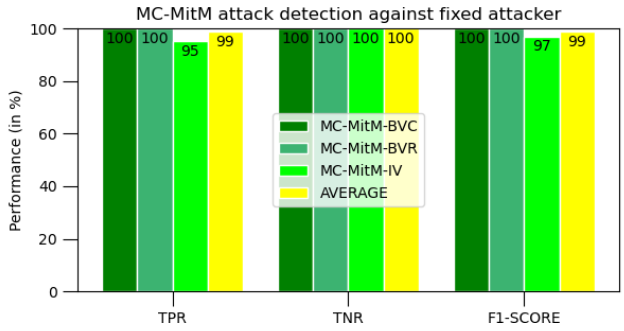


Fig. 11 Detection performance achieved with DC-SWIDS framework with 3 distributed ADS nodes in the experimental testbed against any fixed attacker

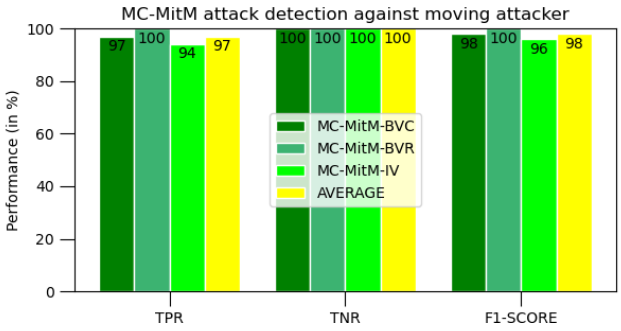


Fig. 12 Detection performance achieved with DC-SWIDS framework with 3 distributed ADS nodes in the experimental testbed against any moving attacker

5.5 Results and discussion: Performance evaluation of DC-SWIDS framework in a Wi-Fi or IoT environment

Fig.11 and Fig.12 respectively showcase detection performance achieved by distributed ADS of our DC-SWIDS framework against fixed and moving attacker locations.

As demonstrated in Fig.11, our DC-SWIDS framework achieves an average True Positive Rate (TPR) of over 99% against fixed attackers. Similarly, Fig.12 illustrates that the framework maintains an average TPR of 97% against moving attackers. These results ensure that the DC-SWIDS framework is not only satisfactory at identifying stationary attackers, but is also capable of adapting to and intercepting attacks that employ mobility as a tactic to complicate detection. Furthermore, as discussed in previous section, our DC-SWIDS framework demonstrated good reliability in accurately identifying attacks with a 100% TNR and achieved good F1-scores (exceeding 98%) in all test cases. Moreover, we also evaluated the DC-SWIDS framework's detection capabilities when operating with fewer ADS nodes than the optimal number, which is identified as three in our targeted experimental testbed. Thus, we conducted an analysis to assess the impact on performance of having fewer deployed nodes. Fig.13 presents the performance results of MC-MitM attack detection using the DC-SWIDS framework with a varying number of ADS nodes.

As we can see from Fig.13, a single ADS node results in lower detection rates, with an average performance hovering around 82%, while the use of two ADS nodes enhances the average detection rate to approximately 94%. However, optimal results are observed with the deployment of three ADS nodes, as recommended by our maximum distance, where the system achieves an average TPR of nearly 99%. This shows that deployment of an optimal number of ADS nodes

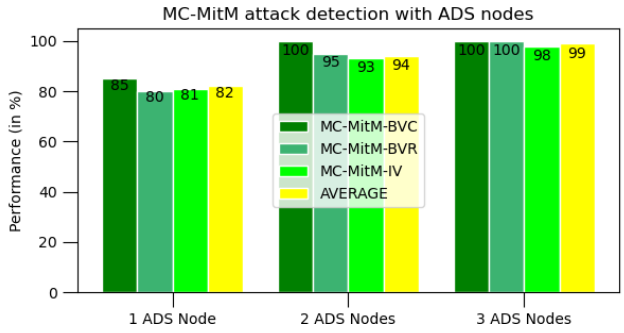


Fig. 13 Detection performance achieved with DC-SWIDS framework with different no. of ADS nodes

has significantly reduced the issue of frame loss while detecting different MC-MitM attacks.

5.6 Comparison of DC-SWIDS with current defense mechanisms

In this section, we compare our proposed DC-SWIDS framework with existing state-of-the-art defense mechanisms, particularly focusing on their efficacy in combating MC-MitM attacks. This comparison builds upon the comparison outlined in our previous paper [15].

For comparative purposes, we utilize a range of criteria to compare different defense mechanisms, including: (1) the capability to detect MC-MitM attacks on WPA/2 clients (□), WPA3 clients (■), or both (○); (2) the capability to detect MC-MitM attacks on PMF-capable clients (□), non-PMF-capable clients (■), or both (○); (3) the capability to detect insider MC-MitM attacks (□), outsider MC-MitM attacks (■), or both (○); (4) the capability to detect (□) or both detect and prevent (○) MC-MitM attacks; (5) the capability to identify MC-MitM attack variant (○) or not (■); (6) requirements for protocol or firmware modifications (□), integration of software/hardware (■), or no modifications (○) for implementation; (7) the capability to provide backward compatibility (○) or lack thereof (■); (8) Applicable to both personal Wi-Fi networks (□), enterprise networks (■), or both (○); the capability to monitor multiple APs simultaneously (○) or not (■), and the capability to monitor multiple wireless channels simultaneously (○) or not (■). These comparisons are summarized in Table 3. The presence of more open circles (i.e., icon ○) in the row of a specific defense mechanism indicates greater effectiveness in detecting MC-MitM attacks.

Table 3 reveals that the DC-SWIDS framework is adept at identifying threats across all device types within WPA2/3 networks, including those PMF-capable. It efficiently counters both insider and outsider threats and various MC-MitM attack variants. Notably, DC-SWIDS maintains backward compatibility, requires no modifications to protocols or devices, and is user-friendly. Its capability to monitor multiple APs and channels in both personal and enterprise networks, coupled with passive attack signature detection, positions DC-SWIDS as a superior solution that enhances security against MC-MitM attacks, outperforming existing defense mechanisms. At the same time, we also want to note that currently we do not incorporate any protection mechanism for MC-MitM attacks, as prevention is not feasible on a large scale in the short term, our work lays the foundation by providing a mean to identify and respond to MC-MitM attacks effectively.

5.7 Performance Overhead Evaluation

In this section, we evaluate the performance overhead of the proposed DC-SWIDS framework in detecting MC-MitM attacks. We specifically focus on two key aspects: CPU and memory, and network overhead. Through systematic testing, our aim is to gauge the efficiency of the framework in terms of resource utilization. These insights will be instrumental in determining the framework's suitability for deployment on single-board computers and across various network environments.

5.7.1 CPU, Memory, and Disk Consumption

To evaluate the impact of our defense mechanism on system resources, including CPU, memory, and disk consumption, we executed an analysis using a Raspberry Pi (4b Model, equipped with a 64-bit ARMv8 microprocessor and 2GB of RAM) that runs our autonomous detection system (ADS). Specifically, our analysis focused on tracking the CPU, memory, and disk consumption over a set period of time—in this instance, 300 minutes (5 hours)—to observe the resource demands of the ADS both when idle and during active monitoring. The results concerning CPU, memory, and disk space consumption are respectively depicted in Fig.14, Fig.15, and Fig.16.

5.7.2 Network Overhead

In order to test the network overhead of our proposed system, especially as part of cooperative communication, we conducted an experiment in which we measured how many bytes of MQTT messages have been transmitted or exchanged in previous N seconds (in our case, we used 300 seconds (1 hour)) on each ADS distributed in a targeted Wi-Fi network (with 50 Mbps of data bandwidth on the network interface) during the running period. Fig.17 illustrates the average bytes of MQTT traffic or network packets being exchanged with four ADSs.

Table 3 Comparative analysis of proposed DC-SWIDS with current defense mechanisms

Defense mechanism/ Metrics	Capable to detect MC-MitM targeting WPA2/3 clients	Capable to detect MC-MitM targeting PMF capable /incapable clients	Capable to detect insider/outsider MC-MitM	Capable to detect and/or prevent MC-MitM	Capable to identify MC-MitM attack variant	Protocol/ device changes	Capable to provide backward compatibility	Applicable to both personal and enterprise Wi-Fi	Capable to monitor multiple APs simultaneously	Capable to monitor multiple channels simultaneously
Proposed DC-SWIDS framework	○	○	○	□	○	○	○	○	○	○
SWIDS framework [15]	○	○	○	□	○	○	○	○	■	■
OCV [17]	■	□	○	○	■	□	■	○	■	■
Beacon Protection [18]	■	□	■	○	■	□	■	○	■	■
Stupify [22]	□	■	■	□	■	□	■	□	■	■
SSAD [24]	□	■	○	□	■	■	■	□	■	■
SAE-PK [20]]	■	□	■	○	■	□	■	□	■	■

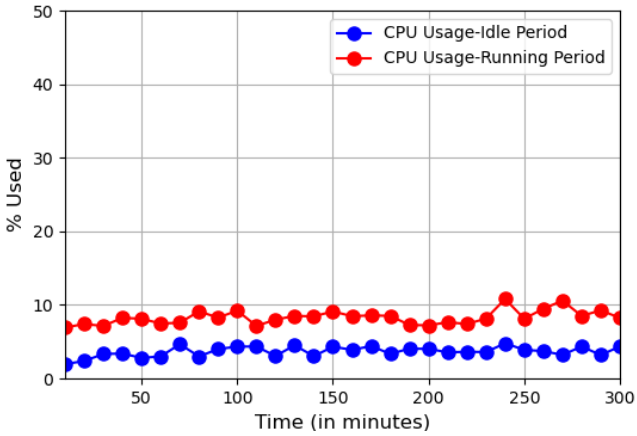


Fig. 14 Resource utilization involving CPU consumption

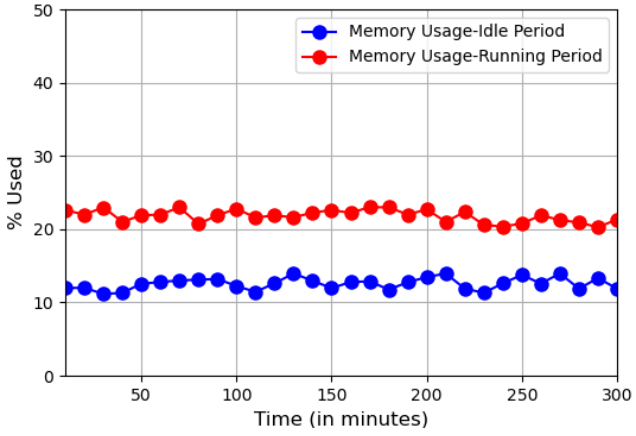


Fig. 15 Resource utilization involving memory consumption

5.7.3 Discussion on Performance Overhead

Fig.14 illustrates a nominal increase in CPU consumption, averaging only 5% after the activation of an ADS within our DC-SWIDS framework. This increase is primarily attributed to the processes involved in capturing Wi-Fi frames and subsequent extraction of data. Memory consumption, as shown in Fig.15, experiences an average augmentation of 12% (approximately 0.48GB) when an ADS node is operational. This minor increase is attributed to the storage requirements for the number of identified malicious frames and the corresponding attack traffic status during each probe interval. Moreover, the disk consumption, represented in Fig.16, is considerably low, which can be attributed to the storage of alerts in a compact text file format. Additionally, analysis of network traffic, as detailed in the network usage graph (see Fig.17), trans-

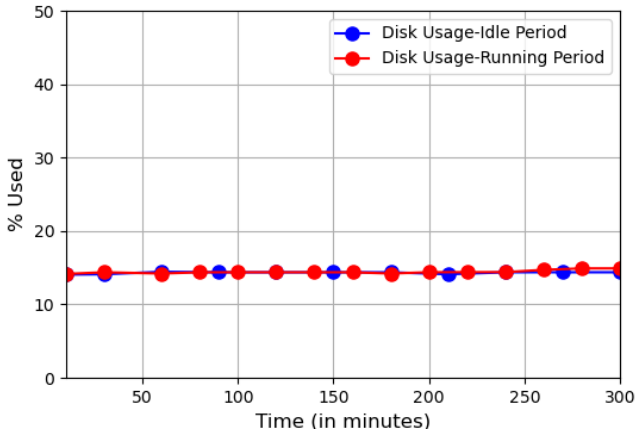


Fig. 16 Resource utilization involving disk consumption

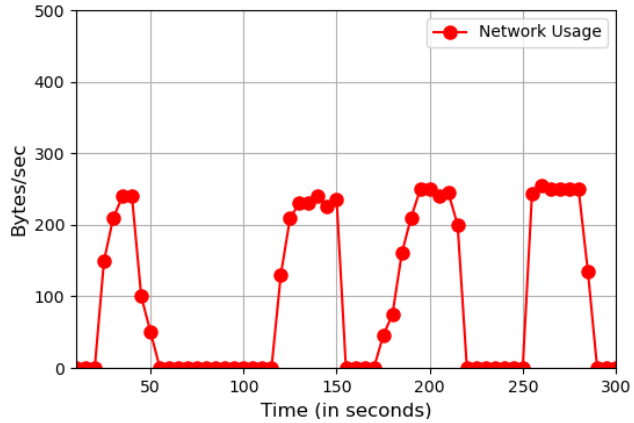


Fig. 17 Network overhead during cooperative communication

mits only around 200 bytes on average during an attack. In addition, there is no MQTT traffic when there is no attack, indicating that there is no unnecessary cooperative communication. This reveals that the ADS node's activity does not exert a significant impact on network load, which is essential for maintaining optimal network performance. Collectively, these findings indicate that the ADS node designed for the DC-SWIDS framework functions with minimal impact on system resources. Hence, it constitutes an efficacious yet resource-efficient security solution, well-suited for diverse deployment contexts, and can be reliably implemented on devices with constrained resources such as the Raspberry Pi.

5.8 Security Considerations

Our DC-SWIDS framework identifies MC-MitM attacks and is applicable to all Wi-Fi networks and devices. Leveraging passive monitoring techniques, the framework exhibits proficiency in identifying both insider and outsider MC-MitM attacks to any Wi-Fi-enabled device. Notably, the framework presents significant challenges for potential attackers seeking to bypass its defenses, even those with knowledge of the specific defense mechanisms and algorithms implemented. This robustness is attributed to the establishment of detection thresholds grounded in both theoretical and empirical analyses of Wi-Fi protocol operations, effectively rendering it infeasible to execute such attacks without exceeding these predefined thresholds (see Table 1 in our previous paper [15]).

The proposed DC-SWIDS framework enables the deployment of multiple ADS nodes to concurrently monitor either a single or multiple APs across various wireless channels. This adaptability enhances the framework's ability to provide comprehensive security surveillance tailored to specific needs, significantly mitigating frame loss and accelerating the detection of attacks throughout the monitored region. In this framework, the distributed ADS nodes utilize TLS-secure and authenticated MQTT communication for data exchange (see Section 3.1). This approach ensures that the DC-SWIDS framework can effectively prevent potential attackers from setting up unauthorized ADS nodes or from intercepting and decrypting vital information, even if they manage to infiltrate the network.

Our framework is designed for easy, plug-and-play deployment, eliminating the need for any modifications to the protocols or devices used by Wi-Fi clients and access points (APs). This plug-and-play functionality necessitates only the SSID of the Wi-Fi network being monitored against MC-MitM attacks. The inherent simplicity of our approach ensures that typical users can enact our detection mechanism without confronting considerable technical hurdles, making it highly accessible for widespread implementation. Additionally, our framework is scalable, allowing for the effortless addition of more ADS nodes to enhance coverage against MC-MitM attacks. For instance, to incorporate an extra ADS node, a user can easily set up a pre-configured ADS node, such as a Raspberry Pi, by configuring the network name via a graphical user interface (GUI). Importantly, our distributed framework's design ensures that if any ADS node encounters issues, such as network congestion or delays, the remaining nodes will continue to collaborate effectively in detecting MC-MitM attacks.

6 Conclusions and future work

In this work, we introduced a distributed and collaborative wireless intrusion detection system designed to detect various MC-MitM attack variants. We developed this system using Scapy, a Python library for network packet capture and manipulation, along with MQTT for node communication, and utilized standard wireless interfaces. This system seamlessly integrates into Wi-Fi-based IoT environments and operates independently of any specific Wi-Fi protocols or standards, requiring no alterations to current network configu-

rations or hardware. It provides robust, ongoing protection from MC-MitM attacks, which are critical in the context of broader security threats such as KRACK and FragAttacks. We assessed the effectiveness of our DC-SWIDS framework by conducting tests against actual MC-MitM attacks within a specially configured experimental environment, closely monitoring the detection capabilities across various distributed ADS nodes. Our results showed that the proposed distributed framework efficiently manages potential frame losses and detects MC-MitM attacks with a minimum average accuracy of 98% when distributed at different locations following the recommended maximum separation between ADS nodes. As a future work, we plan to implement our framework as an installable plugin for smart home domotics such as Home Assistant or OpenHAB.

Funding: This work is linked to the SERCURING project PID2021-125962OB-C31, funded by the Ministerio de Ciencia e Innovación, la Agencia Estatal de Investigación and the European Regional Development Fund (ERDF), as well as the ARTEMISA International Chair of Cybersecurity and the DANGER Strategic Project of Cybersecurity, both funded by the Spanish National Institute of Cybersecurity through the European Union - NextGenerationEU and the Recovery, Transformation and Resilience Plan.

Declarations

Compliance with Ethical Standards: This study does not engage human participants or animals, hence ethical issues pertaining to human or animal subjects are not relevant for this paper

Competing Interests: The authors declare that they have no competing interests.

Acknowledgements The authors would like to express their gratitude to Mathy Vanhoef for his assistance with source codes and his help in addressing certain problems associated with MC-MitM attacks.

References

1. B Fajar. Fluxion kali linux tutorial, 2017. Accessed Feb 29, 2024, (2017, July 21). from : https://linuxhint.com/fluxion-kali-linux-tutorial.
2. Aircrack-Ng . airbase-ng [aircrack-ng], 2018. Accessed Feb 29, 2024, (2018, March 11). from : https://www.aircrack-ng.org/doku.php?id=airbase-ng.
3. Mathy Vanhoef and Frank Piessens. Advanced wi-fi attacks using commodity hardware. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 256–265, 2014. https://doi.org/10.1145/2664243.2664260.
4. Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues. Multi-channel man-in-the-middle attacks against protected wi-fi networks: A state of the art review. *Expert Systems with Applications,Elsevier*, 210:118401, 2022. https://doi.org/10.1016/j.eswa.2022.118401.
5. Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues. Multi-channel man-in-the-middle attacks against protected wi-fi networks and their attack signatures. In *International Conference on Computer, Communication, and Signal Processing*, pages 269–285. Springer, 2023. https://doi.org/10.1007/978-3-031-39811-7_27.
6. Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 1313–1328, 2017. https://doi.org/10.1145/3133956.3134027.
7. Mathy Vanhoef. Fragment and forge: breaking {Wi-Fi} through frame aggregation and fragmentation. In *30th USENIX security symposium (USENIX Security 21)*, pages 161–178, 2021.
8. Wi-fi alliance, 2020. Accessed Feb 25, 2024, (2020, June 18). from : http://surl.li/siwfe.
9. Philipp Ebbecke. Protected management frames enhance wi-fi® network security, 2020. Accessed Feb 25, 2024, (2020, Jan 30). from : http://surl.li/siweq.
10. Benjamin Bertka. 802.11 w security: Dos attacks and vulnerability controls. In *Proc. of Infocom*, 2012.
11. Mathy Vanhoef. Fragattacks: Clarifying some aspects, 05 2021. Accessed Feb 25, 2024, (2021, March 05). from : https://www.mathyvanhoef.com/2021/05/fragattacks-clarifying-some-aspects.html.
12. CWNP. Wireless lan security and ieee 802.11w, 2009. Accessed Feb 25, 2024, (2021, March 05). from : https://www.cwnp.com/wireless-lan-security-and-ieee-802-11w.
13. Constantinos Louca, Adamantini Peratikou, and Stavros Stavrou. 802.11 man-in-the-middle attack using channel switch announcement. In *Selected Papers from the 12th International Networking Conference: INC 2020 12*, pages 62–70. Springer, 2021.
14. MTROI. Protected management frames (802.11w), 2014. Accessed March 25, 2024, (2014, Sept 05). from : https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w.
15. Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues. A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected wi-fi networks. *IEEE*

Access, 2024. https://doi.org/10.1109/ACCESS.2024.3362803.

16. Manesh thankappan. Dcswids framework for detecting mc-mitm attacks, 2024. Accessed April 02, 2024, (2024, March 31). from : https://github.com/maneshthankappan/DC-SWIDS_Framework.
17. Mathy Vanhoef, Nehru Bhandaru, Thomas Derham, Ido Ouzieli, and Frank Piessens. Operating channel validation: Preventing multi-channel man-in-the-middle attacks against protected wi-fi networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 34–39, 2018. https://doi.org/10.1145/3212480.3212493.
18. Mathy Vanhoef, Prasant Adhikari, and Christina Pöpper. Protecting wi-fi beacons from outsider forgeries. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 155–160, 2020. https://doi.org/10.1145/3395351.3399442.
19. Mengchao Chi, Bing Bu, Hongwei Wang, Yisheng Lv, Shengwei Yi, Xuetao Yang, and Jie Li. Multi-channel man-in-the-middle attack against communication-based train control systems: Attack implementation and impact. In *Proceedings of the 4th International Conference on Electrical and Information Technologies for Rail Transportation (EITRT) 2019: Rail Transportation Information Processing and Operational Management Technologies*, pages 129–139. Springer, 2020.
20. Nehru Bhandaru Thomas Derham. Sae public key, 2020. Accessed March 01, 2024, (2019, March 10). from : http://surl.li/siwfo.
21. Huawei, 2020. Accessed March 15, 2024, (2020, Jan 10). from : https://support.huawei.com/enterprise/en/doc/EDOC1100008282/b27702df/understanding-wlan-security-policies.
22. Urbi Chatterjee, Rajat Sadhukhan, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Debashis Mahata, and Mukesh M. Prabhu. Stupify: a hardware countermeasure of kracks in wpa2 using physically unclonable functions. In *Companion Proceedings of the Web Conference 2020*, pages 217–221, 2020. https://doi.org/10.1145/3366424.3383545.
23. Armin Babaei and Gregor Schiele. Physical unclonable functions in the internet of things: State of the art and open challenges. *Sensors*, 19(14):3208, 2019. https://doi.org/10.3390/s19143208.
24. Sheng Gong, Hideya Ochiai, and Hiroshi Esaki. Scan-based self anomaly detection: client-side mitigation of channel-based man-in-the-middle attacks against wi-fi. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1498–1503. IEEE, 2020. https://doi.org/10.1109/COMPSAC48688.2020.00-43.
25. Tommy Chin and Kaiqi Xiong. Krackcover: A wireless security framework for covering krack attacks. In *Wireless Algorithms, Systems, and Applications: 13th International Conference, WASA 2018, Tianjin, China, June 20-22, 2018, Proceedings 13*, pages 733–739. Springer, 2018.
26. Yi Li, Marcos Serrano, Tommy Chin, Kaiqi Xiong, and Jing Lin. A software-defined networking-based detection and mitigation approach against krack. In *ICETE (2)*, pages 244–251, 2019.
27. ST Naitik, L Raiton, V Pradnya, and S Vamshi. Mitigation of key reinstallation attack in wpa2 wi-fi networks by detection of nonce reuse. *International Research Journal of Engineering and Technology (IRJET)*, 5(5), 2018.
28. Securingsam . securingsam/krackdetector, 2017. Accessed March 31, 2024, (2016, Dec 12). from : https://github.com/securingsam/krackdetector.
29. Anand Agrawal, Urbi Chatterjee, and Rajib Ranjan Maiti. Checkshake: Passively detecting anomaly in wi-fi security handshake using gradient boosting based ensemble learning. *IEEE Transactions on Dependable and Secure Computing*, 2023. https://doi.org/10.1109/TDSC.2023.3236355.
30. Efstratios Chatzoglou, Georgios Kambourakis, Christos Smiliotopoulos, and Constantinos Kolias. Best of both worlds: Detecting application layer attacks through 802.11 and non-802.11 features. *Sensors*, 22(15):5633, 2022. https://doi.org/10.3390/s22155633.
31. Sydney Mambwe Kasongo and Yanxia Sun. A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers & Security*, 92:101752, 2020. https://doi.org/10.1016/j.cose.2020.101752.
32. Anand Agrawal, Urbi Chatterjee, and Rajib Ranjan Maiti. Ktracker: Passively tracking krack using ml model. In *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy*, pages 364–366, 2022. https://doi.org/10.1145/3508398.3519360.
33. Efstratios Chatzoglou, Georgios Kambourakis, and Constantinos Kolias. Empirical evaluation of attacks against ieee 802.11 enterprise networks: The awid3 dataset. *IEEE Access*, 9:34188–34205, 2021. https://doi.org/10.1109/ACCESS.2021.3061609.
34. G Abare and EJ Garba. A proposed model for enhanced security against key reinstallation attack on wireless networks. *International Journal of Scientific Research in Network Security and Communication*, 7(3): 21–27, 2019.
35. Rajiv Ranjan Singh, José Moreira, Tom Chothia, and Mark D Ryan. Modelling of 802.11 4-way handshake attacks and analysis of security properties. In *Security*

and Trust Management: 16th International Workshop, STM 2020, Guildford, UK, September 17–18, 2020, Proceedings 16, pages 3–21. Springer, 2020. https://doi.org/10.1007/978-3-030-59817-4_1.

36. Cas Cremers, Benjamin Kiesl, and Niklas Medinger. A formal analysis of {IEEE} 802.11's {WPA2}: Countering the kracks caused by cracking the counters. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1–17, 2020.
37. Domien Schepers, Mathy Vanhoef, and Aanjhan Ranganathan. A framework to test and fuzz wi-fi devices. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 368–370, 2021. https://doi.org/10.1145/3448300.3468261.
38. SNORT. Snort - rule docs, 2018. Accessed March 31, 2024, (2018, Aug 20). from : https://www.snort.org/rule_docs/1-44640.
39. Azar Taufique, Mona Jaber, Ali Imran, Zaher Dawy, and Elias Yacoub. Planning wireless cellular networks of future: Outlook, challenges and opportunities. *IEEE Access*, 5:4821–4845, 2017. https://doi.org/10.1109/ACCESS.2017.2680318.
40. Home Assistant , 2023. Accessed March 31, 2024, (2023, Aug 20). from : https://www.home-assistant.io/.
41. OpenHAB . openhab, 2024. Accessed March 31, 2024, (2024, Jan 13). from : https://www.openhab.org/.

6

Summary of results and publications

Chapter 6

Summary of Results and Publications

This chapter discusses the results of this thesis, along with a list of publications and projects.

6.1 Thesis results and discussion

This thesis aims to contribute to the detection of MC-MitM attacks. It achieves this through an approach that includes a comprehensive review of existing knowledge, theoretical and empirical analysis of attack behaviors, and the practical design of detection systems. Notably, the thesis also explores the practicality of existing defense measures in defending such attacks. The culmination of this research is the development of a Signature-Based Wireless Intrusion Detection System (SWIDS), and its extension into a Distributed and Cooperative SWIDS (DC-SWIDS), which are tested in real testing scenarios.

In **Chapter 2**, we first conducted an in-depth security analysis of protected Wi-Fi networks and provided a comprehensive background on MitM attacks in Wi-Fi environments. Following this, we conducted an evaluation of the capabilities of MC-MitM attacks, delineating their distinct functionalities in manipulating protected Wi-Fi communications when compared to traditional rogue AP MitM attacks. Our exploration includes the classification of MC-MitM attacks, an examination of various related attacks across WPA, WPA2, and WPA3, and a thorough analysis of their security implications. We observed that the effectiveness of MC-MitM attacks is exacerbated by the revelation of key reinstallation vulnerabilities, enabling attackers to decrypt communications from Wi-Fi devices unless adequately patched. Although some patches are available, their applicability to every Wi-Fi device is limited, presenting significant challenges in terms of security patching, particularly evident in IoT devices. The emergence of recent FragAttacks further amplifies the prevalence of MC-MitM attacks, facilitating the injection of genuine packets into protected wireless networks and compromising users' sensitive data. FragAttacks pose substantial challenges and are a significant cause for security concerns. Devices are

likely to remain vulnerable in the foreseeable future due to inadequate implementation of Wi-Fi Alliance patches and the absence of adequate defense mechanisms. We anticipated encountering similar challenges in patching FragAttacks as those experienced with KRACK vulnerabilities.

As far as the defense systems against MC-MitM attacks are concerned, we found that existing mechanisms are inadequate, as many of the mechanisms incorporated by the WFA in 802.11 standards, such as OCV and Beacon Protection, allow certain forms of MitM or insider attacks. Our study highlighted several research issues stemming from design deficiencies within the standards and technical feasibility concerns. Regarding design deficiencies, it is notable that there is a lack of existing solutions aimed at protecting PMF clients from MC-MitM attacks, as these attacks can effectively bypass and disrupt PMF protection measures in various ways. Moreover, MC-MitM attacks pose particular threats when initiated by insiders, such as in the case of fragmentation cache attacks, potentially leading to the compromise of private communications within homes or offices. Existing defense mechanisms are inadequate in addressing such complex scenarios effectively. As for technical feasibility issues, a significant hurdle lies in the practical deployment of existing MC-MitM attack defense mechanisms, especially in IoT contexts, due to the extensive firmware modifications required across all devices, which may not always be feasible to implement. Therefore, defending against MC-MitM attacks remains an ongoing challenge, particularly when viewed from an IoT perspective. In light of these challenges, we proposed the development of lightweight and efficient wireless intrusion detection systems tailored to specifically counter MC-MitM attacks in real Wi-Fi based IoT networks.

In Chapter 3, we presented a theoretical analysis of the network behavior during MC-MitM attacks, leading to the classification of these attacks into stage 1 and stage 2 attack traffic. Stage 1 attack traffic, occurring during the acquisition of the MC-MitM position, exhibited distinct behaviors depending on the attack variant. For instance, MC-MitM-BVC and MC-MitM-BVR attacks manifested as constant jamming and reactive jamming, while MC-MitM-IV attacks were characterized by fake CSAs. Following the acquisition of the MC-MitM position, stage 2 attack traffic emerged, in which the attacker established fake connections and exchanged authentication, association, 4-way handshake frames, and data frames between the client and the legitimate AP. As a future endeavor, the implementation of a wireless intrusion detection system utilizing these attack signatures was proposed.

In Chapter 4, we extended our previous chapter by creating appropriate attack signatures of MC-MitM attacks, which are validated by the empirical evidence from real testing. A reference attack scenario was established to test these signatures for distinguishing between attack traffic and normal traffic. These signatures are based on thresholds that can trigger the detection of various MC-MitM attacks. More specifically, we defined the thresholds for identifying the appearance of malicious frames as part of the essential op-

erations (stage 1 and stage 2 attack traffic) required for successful MC-MitM attacks, and it is impossible to carry out such attacks without meeting or surpassing those thresholds. We have employed a threshold-based approach in order to passively detect these MC-MitM attacks, since this is cost-effective and faster compared to machine learning-based solutions. We then introduced a lightweight, signature-based intrusion detection system aimed at detecting various MC-MitM attack signatures. We devised various network traffic detection algorithms capable of identifying different stage 1 and stage 2 attack traffic of MC-MitM attack variants.

Following the formulation of our framework, we proceeded to implement it using Scapy, a Python library designed for packet capturing and manipulation, in conjunction with commercially available wireless interfaces. Our framework adopts a centralized, passive monitoring approach, facilitating plug-and-play integration with Wi-Fi-based IoT environments. Importantly, it operates independently of specific Wi-Fi protocols or standards, necessitating no modifications to existing network settings or devices. Furthermore, our system offers continuous protection against MC-MitM attacks. We then proceeded to assess the efficacy of our framework through experimentation with real MC-MitM attacks in a configured IoT network environment, focusing particularly on detection performance across varying distances. Our findings revealed that our framework achieves a minimum True Positive Rate (TPR) of 90% with short-distance detectors and 84% with long-distance detectors, exhibiting a maximum detection delay of 60 seconds. Furthermore, we examined the performance of our framework across different channels and channel bandwidths, determining that specific channel selections have negligible impact on detection performance. Additionally, our analysis demonstrated minimal CPU and memory overhead associated with our SWIDS framework, underscoring its suitability for diverse smart home network deployments.

In Chapter 5, we aim to effectively handle the frame loss that affects our previous SWIDS framework, especially with long-distance detectors and to ensure wider surveillance for MC-MitM attacks. Consequently, we proposed a distributed and cooperative wireless intrusion detection system framework (DC-SWIDS) for identifying different MC-MitM attack variants. We mainly extended our SWIDS framework into an Autonomous Detection System (ADS) that can be distributed in a Wi-Fi environment for a wider surveillance against MC-MitM attacks. Furthermore, distributed ADS nodes cooperate by exchanging the status of attack data. This results in quicker detection and allows independent attack decisions in the places where ADS nodes are deployed. We then developed our DC-SWIDS using Scapy, MQTT communication for cooperation between ADS nodes, and commercially available wireless interfaces. We implemented our DC-SWIDS framework on a Raspberry Pi and can be easily integrated with Wi-Fi-based environments for providing continuous security against MC-MitM attacks over wider areas. Through a series of empirical analysis, we identified an optimal maximum distance between distributed

ADS nodes, which can be followed in both residential and commercial environments. We then evaluated our DC-SQUIDS framework with real MC-MitM attacks in an experimental testbed and specifically analyzed detection performance with multiple ADS nodes distributed in a targeted experimental testbed. Our results showed that the proposed distributed framework efficiently manages potential frame losses and detects MC-MitM attacks with a minimum average TPR of 98%.

6.2 List of publications and projects

Four manuscripts have been included in the preparation of this thesis. Three of them have already been published in international scientific journals or conferences and another one is currently under review. In addition, two open source tools and one dataset have been created and made available online for experimentation.

Published journal papers

- **Thankappan, Manesh; Rifà Pous, Helena; Garrigues Olivella, Carles.** *Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review.* Expert Systems with Applications, 2022, vol. 210, pp. 1-29.
  `https://doi.org/10.1016/j.eswa.2022.118401`
  - Impact factor 2023 (JCR): 8.5
  - Quartile: Q1 Computer Science, Artificial Intelligence; Q1 Engineering, Electrical & Electronic; Q1 Operations Research & Management Science
  - Citations (29 April 2024): ISI: 3; SCOPUS: 7; Google Scholar: 22
- **Thankappan, Manesh; Rifà-Pous, Helena; Garrigues Olivella, Carles.** *A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks.* IEEE Access, 2024, vol. 12, pp. 23096-23121.
  `https://doi.org/10.1109/ACCESS.2024.3362803`
  - Impact factor 2022 (JCR): 3.9
  - Quartile: Q2 Computer Science, Information Systems; Q2 Engineering, Electrical & Electronic; Q2 Telecommunications)
  - Citations (29 April 2024): ISI: 0; SCOPUS: 1; Google Scholar: 1

Submitted journal papers

- **Thankappan, Manesh; Rifà-Pous, Helena; Garrigues Olivella, Carles.** *A Distributed and Cooperative Signature-Based Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks.* International Journal of Information Security, Springer. (Under review)
  - Impact factor 2022 (JCR):3.2
  - Quartile: Q2 Computer Science, Software Engineering; Q2 Computer Science, Theory & Methods; Q3 Computer Science, Information Systems)

Published conference papers

- **Thankappan, Manesh; Rifà-Pous, Helena; Garrigues Olivella, Carles.** *Multi-channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks and Their Attack Signatures.* Computer, Communication, and Signal Processing. AI, Knowledge Engineering and IoT for Smart Systems. Editorial: Springer , 28 August 2023, pp. 269-285
  `https://doi.org/10.1007/978-3-031-39811-7_27`
  - Citations (29 April 2024): ISI: 0; SCOPUS: 0; Google Scholar: 0

Open source software

- **Thankappan, Manesh.** *Signature-Based-WIDS-for-detecting-MC-MitM-attacks.* 2023.

  [Online]. Available:

  `https://github.com/maneshthankappan/Signature-Based-WIDS-for-detecting-MC-MitM-attacks`
  - **Description**: This open source software stems from a research paper titled **A Signature-Based Wireless Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks.** We have developed a proof of concept (PoC) for the SWIDS framework using the Python-Scapy library. The software is implemented on a laptop running Kali Linux OS.
- **Thankappan, Manesh.** *DC-SWIDS framework for detecting MC-MitM-attacks.* 2024.

  [Online]. Available:

`https://github.com/maneshthankappan/DC-SWIDS_Framework`

  - **Description**: This open source software stems from a research paper titled **A Distributed and Cooperative Signature-Based Intrusion Detection System Framework for Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks.** We have developed a proof of concept (PoC) of the Autonomous Detection System(ADS) for the DC-SWIDS framework using the Python-Scapy library. The software is implemented on Raspberry Pi Model 4.

Dataset

- **Thankappan, Manesh.** *MC-MitM Attack Signatures.* 2023.

  [Online]. Available:

  `https://github.com/maneshthankappan/-MC-MitM-Attack-Dataset`

  - **Description**: This is a public dataset and is a result of the research paper titled **Multi-channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks and Their Attack Signatures.** We generated this PCAP-based dataset by capturing wireless communications with Wireshark software during various MC-MitM attacks in a controlled setting. Researchers can observe different MC-MitM attack signatures or presence of dubious frames by applying the filters provided on our GitHub page.

List of projects

This PhD thesis has been developed at the **K-riptography and Information Security for Open Networks** (KISON) research group at the Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya, through a doctoral grant from the Doctoral School. During the development of the PhD, I was involved in the development of the following research projects:

- **[INCIBE Chair] International Chair ARTEMISA in Cybersecurity. Chair INCIBE UPF-UOC – Recovery, Transformation and Resilience Plan. Project Period: (2023-2026)**
  `https://www.upf.edu/web/artemisa/`

  - **Description**: The project aims to empower professionals with cybersecurity skills, promote widespread adoption of robust security measures, and advocate for diversity and inclusion in the field, particularly for women. It also seeks

to drive research and development of innovative cybersecurity techniques and tools, ultimately enhancing the overall security landscape of digital environments.

- **[INCIBE Strategic Project] Strategic project DANGER of Cybersecurity. Project INCIBE UAB-UOC - Recovery, Transformation and Resilience Plan.**
  Project Period: (2023-2025)
  `https://proyectodanger.es/`

  - **Description**: This project aims to tackle the growing issue of the dissemination of false or malicious content across networks by utilizing tools that analyze such information and enable its potential malicious identification for subsequent filtering. Focusing on four key topics outlined in the INCIBE's public invitation, the project emphasizes data security, solutions for preventing malicious use of data, innovative systems for IoT device security analysis, tracking systems for crypto-transactions, and innovative cybersecurity solutions for 5G networks.

- **[PID2021-125962OB-C31] Bringing Sustainable Cybersecurity to the Internet of Things (SECURING), Proyectos de Generación de Conocimiento del Ministerio de Ciencia e Innovación.**
  Project Period: (2022-2024)
  `https://crises-deim.urv.cat/securing/`

  - **Description**: SECURING aims to provide cost-effective cybersecurity and privacy technologies to endorse IoT infrastructures with the required levels of protection that are necessary for a sustainable deployment of this technology. This includes proposing new mechanisms for IDP in IoT infrastructures making use of advanced machine learning-based and data provenance solutions using digital watermarking techniques. These intrusion detection and prevention mechanisms will be developed at three different levels, taking into account the following scenarios: IDP at the wireless layer; IDP in cloud-based IoT networks; IDP in IoT vehicular networks.

- **[RTI2018-095094-B-C22] GDPR-compliant CONSumer oriENTed IoT (CONSENT). Proyecto Retos de Investigación del Ministerio de Ciencia, Innovación y Universidades.**
  Project Period: (2019-2023)
  `https://crises-deim.urv.cat/consent/`

  - **Description**: CONSENT aims to provide cost-effective security and privacy technologies to guarantee the data protection levels established by the GDPR. CONSENT will develop security infrastructures that can ensure a reliable in-

terchange and processing of data in IoT consumer environments. To this end, it will:

* Evolve cybersecurity technologies to detect attacks and anomalies in an heterogeneous and resource-constrained context using artificial intelligence algorithms.
* Define protocols for the secure interchange of data based on collaborative peer-to-peer networks and lightweight cryptographic schemes

7

Conclusions and future work

Chapter 7

Conclusions and Future Work

This final chapter summarizes the key contributions of the present thesis and outlines some guidelines for future work.

7.1 Conclusions

This thesis has explored the intricacies of MC-MitM attacks and their impact on Wi-Fi systems, spanning from personal to enterprise networks. These attacks manipulate protected wireless communications between APs and clients, evading standard Wi-Fi security protocols and authentication methods. Our analysis of MC-MitM attacks, including prominent ones like KRACK and FragAttacks, highlights their exploitation of inherent vulnerabilities in the 802.11 standards, affecting a vast number of IoT devices worldwide. The widespread nature of these vulnerabilities emphasizes the urgent need for innovative and practical defense strategies that move beyond traditional solutions, particularly for the diverse array of IoT environments.

In response, this research has proposed a signature-based wireless intrusion detection system (SWIDS). The SWIDS framework introduces a plug-and-play, centralized, passive monitoring system that can be integrated into any Wi-Fi IoT setting. Utilizing lightweight attack signatures, SWIDS effectively identifies MC-MitM activities without requiring changes to existing network protocols or devices. Our system, designed to operate independently of network encryption standards or specific Wi-Fi frequencies, demonstrated high detection accuracy through empirical tests in real testing environments. Achieving a minimum True Positive Rate (TPR) of 90% at short distance and 84% at long distance detectors, SWIDS proved highly effective in various attack simulations while maintaining ease of deployment. The research also identified that frame loss, particularly prevalent at longer distances, significantly influences detection performance. Such frame loss, attributable to network conditions, the time taken to parse and process frames, and the processing capacity of Wi-Fi cards, can lead to the misclassification of some attack incidents as benign traffic.

To enhance detection capabilities and mitigate potential frame loss, this thesis proposed a distributed and cooperative detection strategy within the SWIDS framework, transforming it into a set of Autonomous Detection Systems (ADS) that are uniformly distributed across the detection area. This setup involves deploying multiple ADS nodes across a designated area to minimize frame loss generated from long distances. Additionally, the cooperative strategy enhances responsiveness to MC-MitM attacks by facilitating the exchange of attack data among the deployed ADS nodes. This distributed strategy effectively managed frame losses and consistently maintained a high detection accuracy, achieving at least 98% in identifying MC-MitM attacks in our testing network settings.

To the best of our knowledge, this thesis represents the first effort to conduct an exhaustive review of MC-MitM attacks as documented in the academic literature, analyzing their effects on Wi-Fi systems. The system's practicality and ease of use enable deployment by common users without the need for complex technical interventions, offering effective and continuous protection against the targeted security threats. Consequently, this thesis significantly advances our comprehension of MC-MitM attacks and elevates the state of technological defenses against them.

7.2 Future work

Building on the insights gained from this research, future endeavors are divided into two principal trajectories to further advance the capabilities and applications of our Distributed Cooperative Signature-based Wireless Intrusion Detection System (DC-SWIDS) framework. The first trajectory aims to refine and expand the system development of the Autonomous Detection System (ADS), enhancing its detection accuracy and usability. The second trajectory involves the development of a comprehensive public dataset of MC-MitM attacks to facilitate broader research and development in this field.

Concerning system enhancements, an immediate goal is to automate the network monitoring setup process within the ADS. Future versions will automatically detect and configure the SSID and BSSID of access points to which IoT devices or other network components are connected, eliminating manual entry and reducing setup errors. This automation will streamline the activation process, akin to a plug-and-play system for users. Additionally, we are exploring the integration of support for the emerging 6 GHz frequency band as Wi-Fi 7 technologies become more prevalent. Another significant enhancement will be the implementation of channel hopping algorithms, allowing the ADS to monitor multiple channels simultaneously. This capability will enable comprehensive surveillance of various channels used by single or multiple APs, improving the system's cost-effectiveness and coverage.

For advancements in alert systems, we plan to develop more user-friendly notification mechanisms. All alerts regarding MC-MitM attacks will be communicated through the

add-on application or sent directly to users via SMS, enhancing the accessibility and practicality of the detection system for non-technical users, making it as intuitive as using a standard mobile application.

Regarding the development of a new dataset, our objective is to compile an exhaustive collection of MC-MitM attack scenarios. While our current dataset offers insights into general network behavior during MC-MitM attacks, it lacks detailed data on specific attack types such as KRACK, FragAttacks, DoS attacks, packet size exposing attacks, and various security downgrade exploits. Additionally, the dataset is currently limited to data from APs using Wi-Fi 5 (802.11ac) and 6 (802.11ax) standards. We plan to extend our experiments to include the latest APs supporting Wi-Fi 6E and 7 standards to assess how these modern networks withstand or respond to MC-MitM attacks, particularly examining how Channel Switch Announcements (CSAs) perform under various conditions. This expansion will allow us to refine our dataset with specific AP behaviors and features, providing researchers with detailed attack patterns. This enriched dataset will be instrumental in training sophisticated AI-driven machine learning models that can not only detect the presence of MC-MitM attacks but also identify specific attack vectors, thus enabling network administrators to accurately pinpoint vulnerabilities and implement proactive defenses. These AI models will be particularly valuable in rapidly detecting MC-MitM threats amid the growing number of IoT devices and Wi-Fi access points in industrial and public settings, including Smart Cities. Ultimately, these future directions are designed to enhance the robustness of Wi-Fi network defenses and foster a more secure and resilient digital environment against the evolving landscape of cyber threats.

Bibliography

[1] D. A. Dai Zovi and S. A. Macaulay, "Attacking automatic wireless network selection," in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, IEEE, 2005, pp. 365–372.

[2] B. F. Ramadhan, *Fluxion kali linux tutorial*, 2021. [Online]. Available: `https://linuxhint.com/fluxion-kali-linux-tutorial`, (Accessed Feb 29, 2024).

[3] W. SALAME, *Wifiphisher Evil Twin Attack*, 2019. [Online]. Available: `https://kalitut.com/Wifiphisher-evil-twin-attack/`, (Accessed Jan 10, 2024).

[4] Kalitut, *WiFi Pumpkin framework for Rogue WiFi Access Point Attack*, 2019. [Online]. Available: `https://kalitut.com/wifi-pumpkin-framework-for-rogue-wi-fi/`, (Accessed Feb 29, 2024).

[5] Aircrack-Ng, *Airbase-ng [aircrack-ng]*, 2018. [Online]. Available: `https://www.aircrack-ng.org/doku.php?id=airbase-ng`, (Accessed Feb 25, 2024).

[6] M. Vanhoef and F. Piessens, "Advanced wi-fi attacks using commodity hardware," in *Proceedings of the 30th Annual Computer Security Applications Conference*, `https://doi.org/10.1145/2664243.2664260`, 2014, pp. 256–265.

[7] M. Vanhoef and F. Piessens, "Release the kraken: New kracks in the 802.11 standard," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 299–314.

[8] M. Chi, B. Bu, H. Wang, *et al.*, "Multi-channel man-in-the-middle attack against communication-based train control systems: Attack implementation and impact," in *Proceedings of the 4th International Conference on Electrical and Information Technologies for Rail Transportation (EITRT) 2019: Rail Transportation Information Processing and Operational Management Technologies*, Springer, 2020, pp. 129–139.

[9] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, `https://doi.org/10.1145/3133956.3134027`, 2017, pp. 1313–1328.

[10] M. Vanhoef, "Fragment and forge: Breaking {wi-fi} through frame aggregation and fragmentation," in *30th USENIX security symposium (USENIX Security 21)*, 2021, pp. 161–178.

[11] Google, *Android Security Bulletin*, 2017. [Online]. Available: `https://source.android.com/docs/security/bulletin/2017-11-01`, (Accessed March 25, 2024).

[12] Aruba, *WPA2 Key Reinstallation Vulnerabilities-Aruba Product Security Advisory*, 2017. [Online]. Available: `https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt`, (Accessed March 25, 2024).

[13] O. Santos, *Perspective About the Recent WPA Vulnerabilities (KRACK Attacks)*, 2017. [Online]. Available: https://blogs.cisco.com/security/wpa-vulns, (Accessed March 25, 2024).

[14] CERT, *Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse*, 2019. [Online]. Available: https://www.kb.cert.org/vuls/id/228519, (Accessed Jan 21, 2024).

[15] J. Freudenreich, J. Weidman, and J. Großklags, *Responding to KRACK: Wi-Fi security awareness in private households*. Jan. 2020, pp. 233–243. DOI: 10.1007/978-3-030-57404-8\{_}18. [Online]. Available: https://doi.org/10.1007/978-3-030-57404-8_18.

[16] M. Vanhoef and F. Piessens, "Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys," Aug. 2016, pp. 673–688. [Online]. Available: https://atc.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_vanhoef.pdf.

[17] T. Van Goethem, M. Vanhoef, F. Piessens, and W. Joosen, "Request and Conquer: Exposing cross-origin resource size," Aug. 2016, pp. 447–462. [Online]. Available: https://atc.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_van-goethem.pdf.

[18] W.-F. Alliance, *Technical Note Removal of TKIP from Wi-Fi Devices*, 2015. [Online]. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Alliance_Technical_Note_TKIP_v1.0.pdf, (Accessed Feb 26, 2024).

[19] P. Ebbecke, *Protected Management Frames enhance Wi-Fi network security*, 2018. [Online]. Available: https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security, (Accessed Feb 25, 2024).

[20] M. Vanhoef, *Fragattacks: Clarifying some aspects*, 2021. [Online]. Available: https://www.mathyvanhoef.com/2021/05/fragattacks-clarifying-some-aspects.html, (Accessed Dec 11, 2023).

[21] Gopi, *Wireless LAN Security and IEEE 802.11w*, 2009. [Online]. Available: https://www.cwnp.com/wireless-lan-security-and-ieee-802-11w, (Accessed Jan 11, 2024).

[22] M. Vanhoef, N. Bhandaru, T. Derham, I. Ouzieli, and F. Piessens, "Operating channel validation: Preventing multi-channel man-in-the-middle attacks against protected wi-fi networks," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, https://doi.org/10.1145/3212480.3212493, 2018, pp. 34–39.

[23] B. Könings, F. Schaub, F. Kargl, and S. Dietzel, "Channel switch and quiet attack: New dos attacks exploiting the 802.11 standard," in *2009 IEEE 34th Conference on Local Computer Networks*, IEEE, 2009, pp. 14–21.

[24] C. Louca, A. Peratikou, and S. Stavrou, "802.11 man-in-the-middle attack using channel switch announcement," in *Selected Papers from the 12th International Networking Conference: INC 2020 12*, Springer, 2021, pp. 62–70.

[25] M. Vanhoef, *KRACKing WPA2 and Mitigating Future Attacks*, 2018. [Online]. Available: http://papers.mathyvanhoef.com/crypto-wac2018-slides.pdf, (Accessed April 11, 2024).

[26] L. Wang and A. M. Wyglinski, "Detection of man-in-the-middle attacks using physical layer wireless security techniques," *Wireless Communications and Mobile Computing*, vol. 16, no. 4, pp. 408–426, 2016.

[27] MTROI, *Protected management frames (802.11W)*, 2014. [Online]. Available: https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w, (Accessed Jan 30, 2023).

[28] S. Gong, H. Ochiai, and H. Esaki, "Scan-based self anomaly detection: Client-side mitigation of channel-based man-in-the-middle attacks against wi-fi," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, https://doi.org/10.1109/COMPSAC48688.2020.00-43, IEEE, 2020, pp. 1498–1503.

[29] SNORT, *POLICY-OTHER WPA2 key reuse tool attempt*, 2021. [Online]. Available: https://www.snort.org/rule_docs/1-44640, (Accessed Dec 30, 2023).

[30] D. Schepers, M. Vanhoef, and A. Ranganathan, "A framework to test and fuzz wi-fi devices," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, https://doi.org/10.1145/3448300.3468261, 2021, pp. 368–370.

[31] M. Vanhoef, P. Adhikari, and C. Pöpper, "Protecting wi-fi beacons from outsider forgeries," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, https://doi.org/10.1145/3395351.3399442, 2020, pp. 155–160.

[32] N. B. Thomas Derham, *Sae public key*, 2020. [Online]. Available: http://surl.li/siwfo, (Accessed Feb 15, 2024).

Annex

Annex 1: About the author

Manesh Thankappan, born on April 10, 1983, in Kottayam, Kerala, India. From a young age, Manesh cultivated a deep passion for teaching, profoundly influenced by a series of inspirational teachers throughout his schooling and higher studies. He earned his B.Tech (Bachelor of Technology) degree in Information Technology from Mahatma Gandhi University, Kerala, in 2006. Throughout his undergraduate studies, Manesh excelled academically, earning proficiency awards in all university examinations and ultimately receiving an academic excellence award from his college. His internships at multinational companies during this period sparked his interest in information security, particularly through elective subjects and a major project focused on developing a network packet analysis tool.

Upon completing his bachelor's degree in February 2006, Manesh began his teaching career as a lecturer in the Faculty of Computer Science and Engineering at the Adi Shankara Institute of Engineering and Technology (ASIET) in Cochin, where he remained until October 2012. It was here that he met his mentor, who profoundly influenced his approach to teaching pedagogies, classroom management, and student engagement. Manesh dedicated himself to mentoring students and leading various projects, contributing significantly to their academic and project success. He actively participated in faculty development programs hosted by companies like Infosys and Wipro, which shaped his implementation of modern teaching and learning strategies. During his time at ASIET, Manesh earned numerous accolades, notably winning a prestigious faculty project development competition hosted by Infosys Technologies. He has also organized several FDP at ASIET.

In June 2009, Manesh joined the Master of Technology (M.Tech) degree in Information Security at the National Institute of Technology Karnataka (NITK), India. During his tenure at NITK, he focused on coursework and projects related to information security, while also cultivating a deep interest in cybersecurity and digital forensics. He secured a one-year internship at the Center for Development and Advanced Computing (CDAC)

in Trivandrum, specifically at the Resource Center for Cyber Forensics (RCCF). During his internship, Manesh earned a diverse array of skills in digital forensics. At RCCF , he collaborated with researchers and developers on live projects. For his master's thesis, Manesh designed a network forensic investigation tool tailored to analyze HTTP and FTP sessions and reconstruct actual network streams. This research project allowed him to apply various network forensic methodologies to detect and investigate malicious activities within computer networks.

After completing his master's degree, Manesh expanded the capabilities of his network forensic investigation tool to encompass additional protocols, including HTTPS, FTPS, P2P, VoIP, and Skype. He also documented his advancements in several papers presented at conferences and published in journals. Returning to ASIET in June 2011, Manesh took on the role of assistant professor in the department of computer science and engineering, where he served until October 2012. During this period, he guided numerous master's students through their project work

He then accepted a position as an assistant professor in the Department of Computer Science and Information at Prince Sattam Bin Abdulaziz University (PSAU), an international public university in Saudi Arabia, where he worked until October 2018. During his tenure at PSAU, he had numerous opportunities to engage with international students and faculty members, primarily focusing on teaching subjects related to information security. He participated in several government-funded projects alongside senior professors. His experiences at PSAU also inspired him to pursue a full-time PhD in cybersecurity.

In October 2018, Manesh was admitted to pursue his Ph.D. in Networks and Information Technologies at the Universitat Oberta de Catalunya (UOC), under the supervision of Dr. Helena Rifà-Pous and Dr. Carles Garrigues. His close collaboration with his Ph.D. advisors greatly enriched his expertise in cybersecurity and network and information technologies. He was a member of the K-riptography and Information Security for Open Networks (KISON) research group at UOC and participated in multiple projects funded by the Spanish Ministry of Education. During his doctoral research, Manesh focused on cybersecurity threats in smart homes and IoT environments, where he identified a sophisticated type of Multi-Channel Man-in-the-Middle (MC-MitM) attack affecting millions of Wi-Fi devices globally. This discovery led him to further investigate MC-MitM attacks and develop a practical intrusion detection system (IDS).

Throughout his Ph.D. program, Manesh engaged in various internships, attended international conferences, and published several articles in well-reputed journals. Following his Ph.D. defense, Manesh plans to advance his academic career by pursuing a postdoctoral fellowship at premier universities.

Annex 2: Portfolio

Courses

Courses	Date
Research Methodologies in Network and Inform. Technologies (UOC)	2018-2019
Research Techniques in Network and Information Technologies (UOC)	2018-2019
Bibliographic reference management (UOC)	2018-2019
Academic Writing (UOC)	2018-2019
Practical Ethical Hacking (TCM Security)	2019
Python for Penetration Testers (Udemy)	2020
Python Network Programming—Build Network automation tools	2020
Introduction to Cybersecurity (Cisco)	2020
Python for Pentesters (Pentester Academy)	2020
Wi-Fi Security and Pentesting (Pentester Academy)	2020
Traffic Analysis: TSHARK Unleashed (Pentester Academy)	2021
Scripting Wi-Fi Pentesting Tools in Python (Pentester Academy)	2021
Network Security Scanning - SCAPY (Udemy)	2021
ICSI — CNSS Certified Network Security Specialist (UK)	2021
Cybersecurity and Networking Fundamentals (Skillsoft)	2024
Digital Forensics Essentials (EC-Council)	2024
Network Defense Essentials (EC-Council)	2024

Certifications

Certificate/Licences	Date
Home Automation System Professional (Bharat Sevak Samaj-Govt. of INDIA, Reg No: 115678)	2019

Workshops (Supported by UOC)

Hands-On Training (2-Month internship) @ Ambit, Cochin	Date
Intrusion Detection and Alarm Systems	2019
Building Management Systems (Smart Home Networks)	2019
Pentesting using Raspberry Pi and ESP 8266	2019
Home Automation Using PLC	2019
Human Machine Interface (HMI), Variable Frequency Drive (VFD)	2019
Internet of Things and Ethical Hacking	2019
IOT and Smart Systems during ICCCSP-23	2023

National/International Conferences (Supported by UOC)

Conference	Date
Cybersecurity Research Network Conference (University of Lleida), Oral Presentation, Spain	2022
COCON-XV-International Hacking and Cybersecurity Conference, Oral Presentation, India	2022
International Conference on Computer, Communication and Signal Processing 2023: Oral Presentation, India	2023

Other Academic Activities

Activity	Date
Research Project Presentation @ KISON,UOC	2022


Universitat
Oberta
de Catalunya