Técnicas de Anonimato para Securizar Redes Móviles Ad Hoc

Oscar Manso
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Email: omanso@uoc.edu

Helena Rifà-Pous
Internet Interdisciplinary Institute
Universitat Oberta de Catalunya
Email: hrifa@uoc.edu

***Resumen*—Las redes móviles ad hoc son redes formadas por la interconexión de terminales inalámbricos que de manera autónoma, sin ninguna administración central, establecen enlaces de comunicación entre ellos. La infraestructura de red la componen los propios terminales de usuarios que actúan de gestores y encaminadores de paquetes. Así, un usuario cualquiera puede conectarse con un terminal remoto a través de una conexión multisalto entre diferentes usuarios. En este tipo de redes tan abiertas, uno de los retos prioritarios es proteger el anonimato de los sujetos y sus localizaciones. En este artículo hacemos un repaso de las técnicas existentes a través de los protocolos que se han propuesto en la literatura, y exponemos los problemas que aun quedan abiertos.**

I. Introducción

La proliferación de dispositivos móviles en el mercado ha hecho surgir nuevos medios de comunicación basados en la creación de redes formadas por terminales de usuarios que se agrupan entre sí de forma esporádica y permiten construir una base de comunicación. Este tipo de redes reciben el nombre de redes móviles ad hoc (MANET) y están tomando especial importancia por ser unas redes que no precisan de infraestructura dedicada, son rápidas de desplegar, pueden proporcionar acceso a la información en entornos aislados y/o conflictivos, y su coste es reducido.

La transmisión de datos en las redes ad hoc se realiza a través de los propios terminales de los usuarios, que actúan como encaminadores de los paquetes. Así, el rango de comunicación de un usuario se extiende más allá del alcance de sus radiaciones electromagnéticas, pudiendo crear enlaces de comunicaciones con nodos remotos. Empero, el hecho de transmitir los datos a través de terminales finales entraña una clara amenaza a la privacidad de los usuarios.

Proporcionar servicios de comunicación anónima es una propiedad muy deseable en redes MANET. Sin embargo la arquitectura particular de las MANET conlleva una serie de características funcionales que son únicas y específicas de este tipo de redes, y que impiden la adopción directa de los esquemas de anonimato diseñados por redes cableadas. En concreto, cabe destacar las siguientes características:

- La autogestión de la red se realiza a través de un medio abierto y susceptible a ataques externos, tanto activos como pasivos. Los enlaces de comunicaciones inalámbricos permiten que los mensajes sean escuchados fácilmente por usuarios que no son sus legítimos receptores.
- La capacidad de la red y la responsabilidad de que ésta funcione está distribuida entre todos sus miembros. Los dispositivos que forman la red son terminales genéricos, con una baja protección física. La probabilidad que algunos de estos terminales sean comprometidos no es irrelevante. Ello implica tener buenos sistemas de detección de intrusiones y gestión de la confianza que permitan proteger a la red de ataques internos.
- La topología de red es dinámica y caótica. En general, los terminales de la red son móviles y su estado en la red es transitorio e irregular. Uno de los principales desafíos en este tipo de entornos es el descubrimiento y mantenimiento de rutas de manera eficiente y anónima.
- Los recursos de la red son limitados. Los terminales tienen una capacidad de proceso, memoria y batería reducidos. El ancho de banda también es limitado, y al utilizar redes inalámbricas los canales de transmisión sufren interferencias y devaneos.

En este artículo definiremos las propiedades que son necesarias para proporcionar comunicaciones anónimas en redes ad hoc, y revisaremos el estado del arte de las técnicas de anonimato propuestas así como las funcionalidades que implementan los diferentes protocolos para MANETs. El resto del artículo está organizado de la siguiente forma. En la sección II introducimos y clasificamos las propiedades de anonimato. A continuación revisamos las soluciones propuestas de anonimato de usuarios (sección III), desvinculación del origen de los mensajes (sección IV), y indetectabilidad de la actividad (sección V). Finalmente, la sección VI presenta los principales problemas abiertos del anonimato en MANETs.

II. Anonimato

En primer lugar definimos las propiedades relacionadas con una comunicación anónima:

1. **Anonimato de los sujetos**: propiedad de no ser identificable entre un conjunto de sujetos.
2. **Desvinculación de mensajes**: propiedad de ocultar la relación que hay entre una comunicación y los sujetos que la llevan a cabo.
3. **Indetectabilidad**: incapacidad de distinguir si un elemento existe o no. Si consideramos mensajes, la indetectabilidad supondría que éstos no son suficientemente discernibles de, por ejemplo, ruido blanco.

Las propiedades de anonimato de una red pueden ser violadas por diferentes ataques, tanto activos como pasivos. En los ataques activos los usuarios maliciosos participan en el protocolo de red al que pretenden quebrantar, ya sea a través de ataques externos (como usuarios ajenos al sistema) o ataques internos (como miembros lícitos de la red). Por otro lado, los ataques pasivos no perturban el normal funcionamiento de los protocolos de red, los atacantes escuchan de forma no-autorizada los paquetes que se transmiten por la red y a través de un análisis de tráfico extrapolan información como las rutas de transmisión, el contenido de los mensajes, o la identidad, posición o movimiento de los nodos.

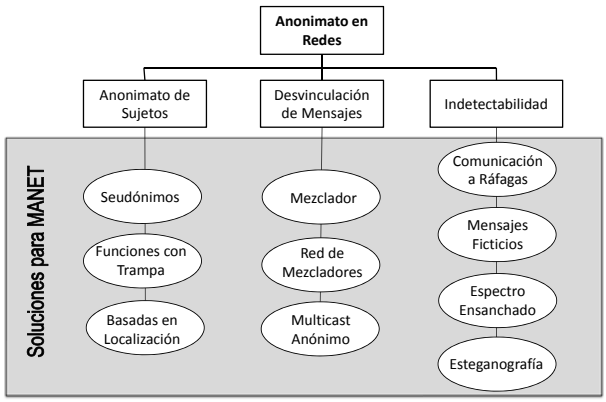

Figura 1. Taxonomía de las técnicas de anonimato para MANETs

En la figura 1 mostramos una taxonomía de las técnicas de anonimato para MANETs: los rectángulos simbolizan las propiedades de anonimato, y las elipses el tipo de soluciones que se han propuesto en la literatura. En los siguientes apartados analizaremos con más detalle las propiedades de anonimato y las soluciones propuestas. La tabla I hace un resumen de las principales soluciones adoptadas por los diferentes protocolos de anonimato en MANET.

	Anonimato sujetos			Desvincul. mensajes		Indetectabilidad
Protocolo	Sinon.	FTramp.	Loc.	Casc.	RLibre	MFict.
R-AO2P [20]	S	-	S	S	-	-
MASK [23]	S	-	-	-	S	Destino
ANODR [14]	S	S	-	S	-	-
ASR [24]	S	S	-	S	-	S
ANONDSR [18]	-	S	-	S	-	S
D-ANODR [21]	S	-	-	S	-	-
ARM [17]	S	S	-	S	-	S
ARMR [11]	S	S	-	-	S	S
ODAR [19]	S	-	-	S	-	-
SDAR [3]	-	S	-	S	-	-
ALARM [8]	S	-	S	S	-	-
PRISM [9]	-	-	S	S	-	-
ANAP [6]	S	S	-	S	-	S
RIOMO [15]	S	-	-	S	-	S
SDDR [12]	-	S	-	S	-	-

Cuadro I
CARACTERÍSTICAS DE LOS PROTOCOLOS DE ANONIMATO PARA MANET

III. ANONIMATO DE LOS SUJETOS

En este apartado se introducen las tecnologías que permiten proporcionar anonimato a los sujetos. Cada una de ellas acomete unos usos específicos de la red.

- **Seudónimos**: Usados como identificadores anónimos de los nodos de un vecindario. Facilitan las comunicaciones salto-a-salto, y que sobre éstas se construyan rutas multisalto.
- **Funciones unidireccionales con trampa** (*Trapdoor functions*): Permiten la búsqueda de nodos anónimos remotos. Se usan en la fase de descubrimiento de rutas de las MANET.
- **Rutas basadas en la localización**: Permite crear rutas anónimas entre nodos situados en puntos concretos de la red.

III-A. Seudónimos

Una forma de esconder la identidad de los sujetos que actúan en una comunicación es a través de seudónimos. Éstos fueron introducidos en 1985 por Chaum [4] como una etiqueta privada que permite, de forma discrecional, distinguir a los participantes de una transacción. A partir de la información pública de la red, los nodos son incapaces de generar y/o vincular seudónimos para el resto de miembros de la red.

Las dificultades que atañe poner en funcionamiento un sistema de seudónimos son:

- Temporalidad: los seudónimos se tienen que renovar periódicamente porque su uso revela cierta información que se podría utilizar para identificar o localizar un sujeto.
- Generación y gestión de los seudónimos: el vínculo entre un seudónimo y la identidad real del sujeto o enlace al que está asociado es privada. Sin embargo, se deben proporcionar mecanismos para hacer llegar esta información a los usuarios autorizados de forma que la comunicación entre entidades sea viable.
- Autenticación: la autenticidad de los participantes en una transacción tendría que poder ser garantizada aunque se usasen seudónimos.

Los sistemas de seudónimos más comunes son los que utilizan una tercera entidad de confianza (TTP) responsable de generar, renovar, revocar y autenticar, los seudónimos [23], [6], [15], [7], [13]. MASK [23] sólo requiere de una TTP para distribuir las claves iniciales del sistema. Sus seudónimos son generados en base a técnicas criptográficas por pares bilineares [2], y se distribuyen fuera de línea, antes de empezar la sesión ad hoc. Los seudónimos iniciales sirven para establecer la autenticación mutua entre dos nodos, momento a partir del cual generan una lista de seudónimos y claves de enlace. La debilidad de este esquema es que se consumen considerables recursos para almacenar la información de los seudónimos (cada nodo debe disponer de un buen grupo de seudónimos ya que cada uno es solo válido para la comunicación con un vecino).

El esquema RIOMO [15] propone un sistema similar a MASK pero más eficiente, ya que los nodos pueden autogenerar sus seudónimos. Inicialmente una TTP distribuye un seudónimo raíz a todos los nodos con una clave secreta asociada. A partir de estos datos cada nodo puede generar seudónimos válidos en la red. Como MASK, RIOMO no protege la identidad del destino en los procesos de descubrimiento de rutas. Por otro lado, el sistema es poco robusto a ataques de tipo Sybil, en los que un nodo adopta varias identidades con el objetivo de participar en múltiples comunicaciones paralelas por la red y obtener más información de la topología de la misma. Ni tan solo la TTP puede tracear la relación entre los seudónimos usados en la red y los identidad real de los nodos.

Para solventar este aspecto y facilitar la autogeneración de seudónimos únicos, el esquema SPS [7] adopta un esquema jerárquico que permite que los nodos generen y revoquen sus propios seudónimos, pero impide que cada nodo tenga más un seudónimo válido durante un intervalo de tiempo. El usuario posee unas claves y certificados generados por una CA externa que son almacenados en un dispositivo *tamper-proof*. A partir de estas claves, que constituyen el nivel superior del esquema jerárquico, el usuario puede generarse unos seudónimos de segundo nivel cada vez que se necesario.

Huang propone un esquema criptográfico basado en seudónimos (*Password-based encryption*, PBE) [13], que es una versión anónima de la criptografía basada en identidades (*Identity-based encryption*, IBE). De forma análoga a IBE, los seudónimos del PBE son usados como las claves públicas de los nodos. Los nodos autogeneran los seudónimos y las correspondientes claves privadas de forma totalmente autónoma, basándose en un conjunto de parámetros públicos del sistema. Para proporcionar servicios de autorización al sistema, Huang indica que los seudónimos pueden ser certificados de forma ciega por una TTP.

Otros esquemas de generación de seudónimos no consideran el aspecto de la autorización de usuarios, y por lo tanto, el sistema es mucho más simple. Este es por ejemplo el modelo usado en ANODR [14]. En lugar de trabajar con seudónimos de identidad, ANODR utiliza seudónimos de ruta que se asocian a los enlaces salto a salto de una red ad hoc. Los seudónimos se establecen en la fase de respuesta de una acción de descubrimiento de rutas. Cada nodo genera un número aleatorio que será usado para identificar el enlace entre él, y el nodo previo de la ruta (posterior en la fase de respuesta). Los seudónimos de un enlace se pueden renovar periódicamente. Por ejemplo, si emisor y receptor están sincronizados, pueden usar una función unidireccional para derivar un nuevo seudónimo cada cierto tiempo.

III-B. Funciones unidireccionales con trampa

La funciones unidireccionales con trampa (*trapdoor functions*) son funciones unidireccionales $f : X \rightarrow Y$ tales que es fácil obtener $f(x)$ para cualquier $x \in X$, y que permiten el cálculo eficiente de la inversa (encontrar $x \in X$ tal que $f(x) = y$) si y solo si se posee cierta información adicional, la trampa. En caso contrario, el cálculo del inverso es computacionalmente intratable.

Las funciones unidireccionales con trampa se utilizan para la identificación anónima de los receptores de una comunicación. El emisor envía la información de identificación de la comunicación escondida en una función trampa, de forma que sólo el receptor legítimo de la transmisión, que posee la información trampa, sea capaz de recuperarla.

La manera más simple de implementar una función unidireccional para proporcionar anonimato de recepción es a través de criptografía de clave pública, como hacen por ejemplo los protocolos SDAR [3], ARMR [11] y AnonDSR [18]. La identidad del receptor se envía cifrada con la clave pública del propio receptor de manera que sólo él pueda abrir con éxito el paquete. Sin embargo, esta solución es muy costosa ya que el descubrimiento de rutas en redes ad hoc se hace a través de mecanismos *broadcast* de inundación, y si todos los nodos que reciben un paquete tienen que hacer una operación criptográfica para descubrir si son los receptores de un paquete, la carga total del sistema es insostenible.

De forma similar a estos últimos, los protocolos ANODR [14] y ASR [24] utilizan criptografía simétrica para esconder la identidad del destino de una comunicación. En este caso se asume que origen y destino comparten una clave TESLA [16]. El origen cifra la identidad del destino y un número aleatorio con la clave simétrica que comparten. El nodo que pueda abrir este sobre y comprobar que su identificador está en él, es el legítimo receptor. Finalmente, en el mensaje de respuesta al origen, el destino envía el número aleatorio del sobre como prueba de recepción de éste.

El protocolo ANAP [6] propone la utilización de funciones trampa más ligeras, basadas en funciones de hash. El origen identifica el destino de la comunicación a través del valor hash de su seudónimo. Sin embargo, los autores no indican cómo puede el origen obtener el seudónimo del destino.

III-C. Rutas basada en la localización

Los autores de ALARM [8] y PRISM [9] utilizan un sistema basado en la localización para establecer rutas con destinos anónimos. Los esquemas son válidos para comunicaciones que se establecen en función de las coordenadas geográficas de los nodos. Es decir, los emisores escogen el receptor no por su identidad, sino por su posición. Este tipo de comunicaciones pueden ser útiles en situaciones de desastre, en redes de vehículos VANET, etc.

Tanto ALARM como PRISM utilizan una TTP externa y fuera de línea para emitir certificados y crear firmas de grupo que ofrezcan autenticidad a los elementos del protocolo sin revelar la identidad de los nodos.

El encaminamiento en R-AO2P [20] también está basado en la localización de los nodos como método para esconder las identidades reales de los usuarios. El descubrimiento de rutas a un determinado destino se hace revelando la posición de un punto de referencia situado en la línea extendida entre el emisor y el receptor. La distancia entre el punto de referencia

y el destino es un valor aleatorio a partir del cual es difícil que un adversario pueda estimar la posición real del destino.

IV. Desvinculación de mensajes

En esta sección analizaremos las técnicas utilizadas para evitar que un adversario pueda inferir los sujetos que participan en una comunicación.

- **Mezclador** (*Mix router*): Encaminador que esconde la correspondencia entre mensajes entrantes y salientes a partir de la modificación de su apariencia y del flujo de la trasmisión.
- **Red de mezcladores** (*Mix network*): Es un conjunto de mezcladores interconectados.
- **Multicast anónimo** (*Anonymous multicast*): Todo mensaje enviado a través de una MANET puede ser recibido por cualquier nodo que se encuentre en su radio de acción. Por tanto, es básico establecer un mecanismo de este tipo para montar un sistema anónimo sobre MANETs.

IV-A. Mezclador

Un mezclador es un encaminador que recibe un conjunto de mensajes de entrada y los devuelve transformados de tal manera que no pueda relacionarse la entrada con la salida. Dichas transformaciones se producen tanto a nivel de forma (a base de aplicar técnicas de encriptación y relleno de mensajes) como de secuencia (a base de mezclar el orden y aplicar distintos retrasos en la entrega de los mensajes).

El diseño original propuesto por Chaum [5] consiste en un mezclador de proceso por lotes que almacena mensajes en la memoria del mezclador hasta que se cumple una cierta condición de descarga, momento en el que se envía el lote de mensajes desordenados. La condición de descarga puede ser una condición temporal, espacial o una combinación de ambas. La descarga temporal se establece cada cierto período de tiempo (que puede ser fijo o variable) mientras que la espacial se establece cuando se llega a sobrepasar un determinado umbral de capacidad.

El diseño original del mezclador por lotes fue extendido más adelante de forma que en el momento de la descarga solo se enviaran un subconjunto de los mensajes almacenados en el encaminador y el resto se preservaran para rondas posteriores. Dicha técnica, llamada mezclador con estanque (Pool Mix), mejora el grado de anonimato en situaciones de tráfico fluctuante a base de compensar un momento de poca carga de tráfico con un mayor retraso en la entrega de los mensajes. Esta solución es ideal para aplicaciones que no tienen restricciones de entrega muy ajustadas, tales como el correo electrónico anónimo.

En contraposición al modelo de mezclador por lotes está el mezclador continuo [10], en el que los usuarios generan un retardo aleatorio por cada mensaje que incluyen en la cabecera del mensaje. El mezclador almacena el mensaje durante el tiempo especificado y entonces lo reenvía. La ventaja de este método es que los propios usuarios controlan el tiempo límite de transferencia de la información. Este modelo funciona bien en situaciones de tráfico relativamente estable y constante. Sin embargo, en caso de que se produzcan períodos de tráfico reducido, el grado de anonimato de este modelo es bajo.

Tanto el mezclador continuo como el de estanque son vulnerables a ataques $N-1$ consistentes en la alteración del flujo de $N-1$ mensajes con el objetivo de poder trazar un mensaje concreto. Para el caso del mezclador continuo el atacante debe ser capaz de bloquear la entrada de mensajes al encaminador, mientras que para el mezclador de estanque tendría que inyectar mensajes marcados que provocaran una descarga controlada del mezclador. Para mitigar el efecto de este ataque, [11] propone que cada encaminador tome la decisión acerca del siguiente nodo sobre el que continuar la ruta, pudiendo incluso llegar a decidir añadir tráfico falso sobre rutas falsas. De hecho, las técnicas de tráfico falso son una buena manera de prevenir dicho problema (ver sección V).

IV-B. Redes de mezcladores

Para incrementar el grado de anonimato de un sistema mezclador, los enrutadores mezcladores suelen combinarse formando una red de mezcladores. De esta manera, puede llegar a preservarse el anonimato de los usuarios aún y cuando algunos nodos de la red sean comprometidos.

Tenemos dos tipologías básicas: Cascadas y mezcladores de Ruta Libre. En una Cascada, la ruta o rutas que siguen los mensajes son preestablecidas. En un mezclador de Ruta Libre, el camino a seguir por cada mensaje puede seguir una ruta independiente.

Una ventaja de las Cascadas sobre los mezcladores de Ruta Libre es el hecho de que tienden a concentrar más tráfico por sus rutas, lo que aumenta el grado de anonimato en las mismas. No obstante, en una Cascada un adversario puede llegar a conocer exactamente qué mezcladores debe controlar para trazar a un usuario en particular. Por tanto, no hay una topología mejor que las otras. Los sistemas [11], [23], [22] implementan el modelo de mezcladores de Ruta Libre, mientras que [1], [20], [14], [24], [18], [21], [17], [19], [3], [8], [9], [6], [15], [12] se ajustan al modelo de Cascada.

Por otro lado, existen modelos de mezcladores combinados que tratan de obtener las ventajas de las dos opciones, como el establecimiento de múltiples Cascadas libres.

Los sistemas de Cascada establecen una única ruta anónima, normalmente la más eficiente, sobre la que pasan todos los mensajes entre fuente y destino. Si se aplican las técnicas de un mezclador, ello puede ser suficiente para garantizar el anonimato de las transmisiones. Sobretodo considerando el hecho de que cualquier mensaje emitido a través de una MANET tiene una naturaleza multicast, lo que aumenta el conjunto de anonimato de los posibles receptores del mensaje.

Sin embargo, en caso de ataque $N-1$ un adversario global podría llegar a trazar una buena parte de la ruta analizando la evolución del tráfico en la red. Para dificultar dicho seguimiento, hay sistemas que extienden la ruta más allá de su destino o que introducen rutas falsas (ver apartado IV-C). Por otro lado, el establecimiento de una única ruta debilita la seguridad del sistema resultante al hacerlo vulnerable a ataques del tipo

rushing (en los que el adversario trata de enviar mensajes de descubrimiento de la ruta antes que el nodo fuente para tratar de «apropiarse» de la ruta) y a intrusiones de un adversario sobre uno de los nodos de la ruta.

Por ello, últimamente se están incorporando más sistemas MANET que permiten el establecimiento de circuitos a través de varias rutas.

IV-C. Multicast anónimo

En una red Ad Hoc todos los mensajes pueden ser considerados de tipo broadcast, ya que éstos pueden ser interceptados por cualquier nodo dentro del área de recepción de la señal electromagnética. Por tanto, todo mensaje enviado a través de dicho tipo de redes debe ser securizado y anonimizado en la medida de lo posible.

De cara a anonimizar los mensajes, una primera medida a tomar es eliminar o distorsionar cualquier referencia identificativa a bajo nivel, es decir, modificando las direcciones MAC de los mensajes y por ejemplo, insertando una sucesión de 1's como direcciones fuente y destino (lo que en 802.11 es indicativo de dirección multicast).

En función de la intencionalidad del emisor, podemos distinguir los siguientes tipos de mensaje:

- Multicast: mensajes dirigidos a todos los nodos en el rango de alcance directo. En su mayoría se trata de mensajes utilizados para iniciar el descubrimiento y/o mantenimiento de rutas. En este caso se trata de mensajes que contienen una parte pública (inteligible para cualquier adversario) y otra privada (utilizada para incorporar parámetros privados de establecimiento de ruta con el nodo destino).
- Unicast: mensajes dirigidos a un nodo en concreto. Son los más utilizados una vez se ha establecido una ruta. Idealmente se trata de mensajes completamente incoherentes e indistinguibles (tanto en su tamaño como contenido) por cualquier nodo que no sea aquel al que el mensaje va dirigido. Por razones de eficiencia, dichos mensajes también pueden llegar a incorporar una parte pública indicando el nodo sobre el que va dirigido el mensaje. Sin embargo, dicho parámetro de direccionamiento debería ser anónimo - es decir, sólo reconocible por el destino del mensaje.

Para evitar que nodos externos a la red puedan reconocer la parte pública de los mensajes, se puede establecer una clave que permita codificar todos los mensajes de la MANET de manera global. Normalmente, por razones de eficiencia, dicha clave global será una clave simétrica. Sin embargo, se ha de tener en cuenta que dicha medida sólo será efectiva mientras que no haya ningún intruso en la red.

Para minimizar el impacto que pueda tener la presencia de intrusos se recomienda tratar de minimizar la información topológica que pueda tener cualquier nodo de la red. Por esta razón - y también por razones de eficiencia -, los algoritmos de descubrimiento reactivos (que establecen la ruta de forma dinámica) acostumbran a ser más populares que los proactivos (en los que algunos nodos de la red son periódicamente alimentados con información topológica por parte del resto de nodos, ver [9] y [8]).

En este sentido es preferible evitar sistemas que apliquen técnicas de Onion Routing (ver Chaum [5]) para el envío de los mensajes anónimos. Ello es debido a que, para la aplicación de dicha técnica, el nodo fuente requiere codificar el mensaje a enviar utilizando N claves, una para cada nodo por los que debe pasar el mensaje. Por tanto, el nodo fuente debe conocer toda la ruta por la que debe pasar el mensaje (SDAR [3],SDDR [12]).

Una alternativa a dicha técnica consiste en el establecimiento de tablas de rutas de seudónimos asociadas a claves y seudónimos destino. Cuando un mensaje llega a un nodo proveniente de un seudónimo fuente, el mensaje es recodificado y enviado al seudónimo destino que marca su tabla. El nodo fuente tiene marcado en la tabla cuál es el seudónimo del primer nodo por el que debe pasar el mensaje para llegar a su destino. Dichas tablas son generadas por cada nodo en el momento de establecer la ruta (ver ANODR [14], ARM [17], ANONDSR [18]) o bien renovadas de forma periódica (MASK [23]).

V. Indetectabilidad

Típicamente las redes anónimas pierden robustez a lo largo del tiempo debido a que un análisis exhaustivo de las trazas de la red permite obtener información de los usuarios y las relaciones que hay entre ellos. Una forma de atacar la raíz de este problema es enmascarar los mensajes entre nodos de forma que un atacante externo no pueda distinguir cuando la red está enviando datos o ruido.

Entre las técnicas más utilizadas para enmascarar los mensajes destacamos:

- **Comunicaciones a ráfagas cortas** (*burst communications*). La transmisión de mensajes muy cortos es muy difícil de detectar por los usuarios externos a la misma. Es por ello que este tipo de transmisiones se utilizan para enviar la información de control más sensible de la red.
- **Envío de mensajes ficticios** (*dummy data*). Su objetivo es conseguir un flujo constante en la red y que el tipo de tráfico (real o falso) sea indiscernible a ojos de un atacante.
- **Modulación por espectro ensanchado** (*spread spectrum*). Las transmisiones por espectro ensanchado se caracterizan porque la información es enviada a través de un ancho de banda mucho más amplio que el mínimo requerido. Las técnicas más usadas son los sistemas de secuencia directa y los sistemas de salto de frecuencia. La ventaja de estos sistemas es que la señal es muy difícil de detectar para usuarios que desconozcan la técnica y la codificación usada para la transmisión del señal.
- **Esteganografía**. Los métodos esteganográficos permiten esconder un mensaje dentro de un flujo de comunicación cualquiera de la red, de forma que solo el receptor legítimo pueda extraer la información del canal. Para el resto de usuario el mensaje es invisible.

De las técnicas para enmascarar mensajes, las más sencilla y usada es la de envío de mensajes ficticios. Los mensajes ficticios pueden ser insertados en la entrada o salida de los

mezcladores. Normalmente la inserción en la salida provee mayor anonimato y menor retraso debido a que el mezclador puede regular de forma más precisa la introducción de mensajes ficticios en la red según el estado del tráfico [14]. Sin embargo, en el caso del ataque $N-1$ la inserción en la entrada del mezclador puede ofrecer un mayor nivel de protección.

Cuando tratamos sobre redes de mezcladores, los Mensajes Falsos pueden atravesar diversos encaminadores, tal como hace el resto de mensajes. El camino a atravesar se determina de forma aleatoria y normalmente termina en el encaminador que lo generó. Ello permite llegar a detectar ataques del tipo $N-1$ y actuar en consecuencia.

En el entorno de redes Ad Hoc, en el que el uso de recursos es muy limitado, el uso de dicho tipo de mensajes debe ser realmente minimizado. Sin embargo, también tenemos la ventaja de que un solo mensaje Falso extiende el conjunto de anonimato entre los posibles receptores a todos los nodos vecinos del nodo que emite dicho mensaje.

VI. Problemas Abiertos

Los principales problemas abiertos en el área de anonimato para redes MANET son los siguientes:

- Anonimato de los sujetos: Uno de los retos principales en esta área consiste en establecer un sistema de confianza que permita la localización y autenticación mutua de nodos que toman la identidad como atributo para seleccionar con quien establecer una comunicación, sin que ello merme el anonimato de dichos nodos frente a usuarios externos. Por tanto, se requiere un protocolo de distribución de las claves iniciales del sistema que sea eficiente y seguro.
- Métodos de incentivo: Debido a la limitada capacidad de los dispositivos deben establecerse mecanismos de incentivo y reputaciones para que los usuarios de una MANET estén dispuestos a proveer sus terminales como enrutadores de mensajes de terceros. Dichos métodos están basados en el establecimiento de protocolos de confianza distribuida, cuyo desarrollo en entornos anónimos es un reto aun no resuelto.
- Desvinculación de mensajes: Área de investigación continua para conseguir protocolos que resulten en una mayor eficiencia y robustez frente a análisis exhaustivo del tráfico.
- Indetectabilidad: Área poco explotada cuya integración con el resto de técnicas a través de soluciónes *cross-layer* podría reforzar el anonimato de los sistemas resultantes.

Agradecimientos

Este trabajo ha sido financiado parcialmente por el Ministerio de Industria, Turismo y Comercio con el proyecto AVANZA TSI-020100-2009-374 SAT2, y por el Ministerio de Ciencia e Innovación y los fondos FEDER con los proyectos TSI2007-65406-C03-03 E-AEGIS y CONSOLIDER CSD2007-00004 ARES.

Referencias

[1] I. Aad, C. Castelluccia, J. P. Hubaux, and G. F. Switzerland. Packet coding for strong anonymity in ad hoc networks. *Proc.of IEEE SecureComm*, 6, 2006.

[2] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[3] Azzedine Boukerche, Khalil El-Khatib, Li Xu, and Larry Korba. An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. *Computer Communications*, 28(10):1193–1203, 2005.

[4] David Chaum. Security without identification: transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, 1985.

[5] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, 1981.

[6] T. Ciszkowski and Z. Kotulski. Anap: Anonymous authentication protocol in mobile ad hoc networks. *Arxiv preprint cs/0609016*, 2006.

[7] Xiaojun Dang and Yang Zhang. Hierarchical pseudonym-based signature scheme and self-generated pseudonym system in ad hoc networks. *Wireless and Mobile Communications, International Conference on*, 0:282–287, 2008.

[8] K. El Defrawy and G. Tsudik. Alarm: Anonymous location-aided routing in suspicious manets. In *IEEE ICNP*. Citeseer, 2007.

[9] K. El Defrawy and G. Tsudik. Prism: Privacy-friendly routing in suspicious manets (and vanets). In *IEEE International Conference on Network Protocols, 2008. ICNP 2008*, pages 258–267, 2008.

[10] C. Diaz and B. Preneel. Taxonomy of mixes and dummy traffic. In *Information security management, education and privacy: IFIP 18th World Computer Congress: TC11 19th International Information Security Workshops, 22-27 August 2004, Toulouse, France*, pages 217–223. Kluwer Academic Pub, 2004.

[11] Ying Dong, Tat Wing Chim, Victor O. K. Li, S. M. Yiu, and C. K. Hui. Armr: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks. *Ad Hoc Networks*, 7(8):1536–1550, 11 2009.

[12] K. El-Khatib, L. Korba, R. Song, and G. Yee. Secure dynamic distributed routing algorithm for ad hoc wireless networks. In *Parallel Processing Workshops*, pages 359–366, 2003.

[13] Dijiang Huang. Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks. *Int. J. Secur. Netw.*, 2(3/4):272–283, 2007.

[14] J. Kong and X. Hong. Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 291–302. ACM New York, NY, USA, 2003.

[15] S. Md, M. Rahman, A. Inomata, T. Okamoto, and M. Mambo. Anonymous secure communication in wireless mobile ad-hoc networks. In *Proceedings of the First International Conference on Ubiquitous Convergence Technology*, pages 131–140. Citeseer, 2006.

[16] Adrian Perrig, Ran Canetti, J.D̃. Tygar, and Dawn Song. The tesla broadcast authentication protocol. *RSA CryptoBytes*, 5(2):2–13, 2002.

[17] S. Seys and B. Preneel. Arm: Anonymous routing protocol for mobile ad hoc networks. *International Journal of Wireless and Mobile Computing*, 3(3):145–155, 2009.

[18] R. Song, L. Korba, and G. Yee. Anondsr: efficient anonymous dynamic source routing for mobile ad-hoc networks. In *Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks*, page 42. ACM, 2005.

[19] D. Sy, R. Chen, and L. Bao. Odar: On-demand anonymous routing in ad hoc networks. In *Proc. of IEEE MASS*, pages 267–276. Citeseer, 2006.

[20] X. Wu and B. Bhargava. Ao2p: Ad hoc on-demand position-based private routing protocol. *IEEE Transactions on Mobile Computing*, pages 335–348, 2005.

[21] L. Yang, M. Jakobsson, and S. Wetzel. Discount anonymous on demand routing for mobile ad hoc networks. In *Proc. of the Second International Conference on Security and Privacy in Communication Networks (SECURECOMM)*. Citeseer, 2006.

[22] Y. Zhang, W. Liu, and W. Lou. Anonymous communications in mobile ad hoc networks. In *IEEE INFOCOM*, volume 3, pages 1940–1951. Citeseer, 2005.

[23] Y. Zhang, W. Liu, W. Lou, and Y. Fang. Mask: Anonymous on-demand routing in mobile ad hoc networks. *IEEE transactions on wireless communications*, 5(9):2376, 2006.

[24] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng. Anonymous secure routing in mobile ad-hoc networks. In *29th IEEE International Conference on Local Computer Networks (LCN)*, pages 102–108. Citeseer, 2004.