IN3 Working Paper Series
INTERNET INTERDISCIPLINARY INSTITUTE
ISSN 2013-8644

A Survey on Security, Privacy and Anonymity in Legal Distribution of Copyrighted Multimedia Content over Peer-to-Peer Networks

Amna Qureshi (aqureshi@uoc.edu)
Helena Rifà-Pous (hrifa@uoc.edu)
David Megías Jiménez (dmegias@uoc.edu)
IN3- Universitat Oberta de Catalunya

Working Paper

Working Paper Series WP13-001

Research group: K-ryptography and Information Security for Open Networks: KISON
Research group coordinator: David Megías Jiménez (UOC)

Submitted in: June 2013
Accepted in: September 2013
Published in: September 2013

Universitat Oberta de Catalunya
IN3 INTERNET INTERDISCIPLINARY INSTITUTE
http://in3.uoc.edu

Internet Interdisciplinary Institute (IN3)
http://www.in3.uoc.edu
Edifici MediaTIC
c/ Roc Boronat, 117
08018 Barcelona
Espanya
Tel. 93 4505200

Universitat Oberta de Catalunya (UOC)
http://www.uoc.edu/
Av. Tibidabo, 39-43
08035 Barcelona
Espanya
Tel. 93 253 23 00

Table of contents

A Survey on Security, Privacy and Anonymity in Legal Distribution of Copyrighted Multimedia Content over Peer-to-Peer Networks

Amna Qureshi (aqureshi@uoc.edu)

Helena Rifà-Pous (hrifa@uoc.edu)

David Megías Jiménez (dmegias@uoc.edu)

IN3-Universitat Oberta de Catalunya

Recommended citation:

QURESHI, Amna; RIFÀ-POUS, Helena; MEGÍAS, David (2013). "Security, privacy and anonymity in legal distribution of copyrighted multimedia content over peer-to-peer networks: A brief overview" [online working paper]. (Working Paper Series; WP13-001). IN3 Working Paper Series. IN3 (UOC). [Accessed: dd/mm/yy].
<url> <http://in3wps.uoc.edu/ojs/index.php/in3-working-paper-series/article/view/n-13-qureshi/n13-qureshi>

Abstract

Recent decades have witnessed a swift development in network structures like Peer-to-Peer (P2P) systems. These P2P systems have some of the advantages that attract users to prefer its usage, such as making the setup running cost very small for the content provider to distribute original content and provide end users to access data within short time. But unfortunately, today's P2P content distribution systems are abused by illegal re-distributions. This illicit activity is not only worrisome for content providers but also for the end-users of these systems. The enforcement of copyright protection mechanisms in P2P content distribution systems poses serious privacy threats to end users, i.e., being monitored for each of their activities within these systems and being held accountable for copyright infringement. Various researchers have examined the challenges characterizing these systems from diverse viewpoints, proposing strategic solutions.

This paper conducts a literature survey of various pertinent studies on the subject with the intention of describing the challenges and solutions that are associated with legal content distribution in P2P systems. To the best of our knowledge, this is the first time a review analysis focused on security, as well as on privacy and anonymity, is conducted.

Keywords

Copyright protection; security; privacy; anonymity; peer-to-peer networks

Introduction

P2P is often described as a type of decentralized computing system in which nodes, referred to as peers, use the Internet to communicate with each other directly. All the peers in this interconnected network provide resources to other peers, including bandwidth, storage space, and computing power. P2P systems are attractive because they do not require any special administrative arrangements, unlike centralized facilities, and their decentralized and distributed nature make them scalable, bandwidth efficient and fault-tolerant.

P2P applications account for approximately 60% of Internet's Traffic. Earlier research efforts in P2P have mainly focused on enabling large scale distributed search. However, in recent decades, a new trend is emerging where P2P systems are considered as an alternative solution to enable large scale content distribution. In particular, today's P2P content distribution applications (eDonkey2000, 2000; gtk-Gnutella, 2000) are extremely popular among millions of users. These applications allow users to contribute, search and obtain a digital content, ranging from relatively small-sized pictures or music files to large-sized contents like complete software packages, movies or similar types of multimedia content, in a distributed manner. Consequently, large amount of data are being shared among these users on a global scale. Content distribution in P2P has also received considerable attention in the research community [Theotokis and Spinellis, 2004; Passarella, 2012].

The P2P technology for content distribution systems is beneficial to both content providers and end users. From media companies and e-commerce vendors' point-of-view, P2P technology enables them to make valuable content available to a large amount of people at minimal cost and better performance as compared to traditional Client-Server distribution systems. Traditional Client-Server content distribution systems are dependent on a centralized server which is costly in terms of initial infrastructure investment and maintenance. Moreover, the lack of scalability and robustness, the server overloading and the high bandwidth requirements, are some factors that degrade the Client-Server system performance. In contrast to Client-Server distribution systems, P2P technology offers cost efficiency (low infrastructure cost), scalability, fault tolerance, less administrative and control requirements and exposure to a large number of users. These benefits of P2P are the attractive features for media companies towards adoption of P2P systems, e.g., BitTorrent [BitTorrent, 2001] is one of the most popular P2P distribution system used on the Internet and it accounts for a significant amount of traffic on the Internet. BBC (British Broadcasting Corporation) uses BitTorrent to distribute hundreds of episodes of various shows. Similarly, Red Hat Inc. uses BiTorrent to

distribute Red Hat Linux. Moreover, BitTorrent has been integrated into some web-browsers such as Opera [Opera, 1996] and Wyzo [Wyzo-The Media Browser, 2010]. Many open source software companies, game companies and new media companies use BitTorrent for distribution of software, game updates and videos respectively. Similarly, Pando Networks [Pando Networks, 2010], a managed P2P content distribution application, enables content owners and media companies to publish, distribute and track their games, video and software at reduced delivery costs. Also, from end users perspective, audio, video and software files can easily be accessed and downloaded within a short time. NBC (National Broadcasting Company) is currently working with Pando Networks to deliver video downloads to end users.

P2P content distribution technology offers content providers (copyright holders) an opportunity to achieve global exposure with low distribution costs as compared to web-based (centralized) content distribution systems. The high distribution costs due to the requirement of powerful processing servers with large storage capacity and administration, high bandwidth consumption and limited capacity expansion of web-based distribution systems (MediaFire [MediaFire, 2006], TransferBigFiles [TransferBigFiles, 2007]) create strong incentives for content providers to adopt lower cost delivery option like P2P technology.

However, despite the potential of P2P content distribution technology to revolutionize the Internet in numerous respects, it has often been surrounded with the copyright controversy. Copyright holders argue that end users of these P2P content distribution systems get copyrighted work and later found to be responsible for illegal re-distribution. Many content providers encounter uncertainties regarding the adoption or rejection of P2P networks to spread content over the Internet. They apparently fear losing control of content ownership in the sense that they are no longer in control of the content distribution and worry about promotion of illegal activity. Also, the decentralized nature of P2P technology makes them more resistive to its adoption due to absence of a central authority, which could regulate how and what kind of files get distributed within the system. Moreover, tracing a copyright violator is an immense task which requires content providers to work in conjunction with watermarking and fingerprinting technology provider firms as well as P2P content distribution service developers. These controversies have been analyzed in [Deewan and Daasgupta, 2010] by authors who summarize that in order to design a secure content distribution system, P2P developers need to identify the gaps in security.

This paper is concerned with the distribution of multimedia files in a merchant-buyer scenario. This means that each content download entails some sort of payment by the recipient of the file (buyer) to the merchant. P2P technology is often used in the private sphere to exchange files (either copyrighted or not) between users without payment. This usage of P2P may be legal or illegal depending on the jurisdiction. Private copying is allowed in some legal environments but forbidden in others. The buyer-seller scenario considered in this paper would be legal everywhere since it would be a replacement of centralized selling systems, such as iTunes.

An illegal re-distribution act is not only onerous to content providers but also to the end users. Users may receive or re-distribute files that may make them accountable to civil or criminal liability under copyright infringement laws. Also, they may receive contents with viruses and other malicious software that could infect their personal computers. Essentially, P2P developers need to examine the security of the system in respect to connection control, operation and the mechanisms for access control [Singh et al., 2004].

In addition to security, another concern among end users is whether the presence of copyright protection mechanism in P2P distribution systems can violate their privacy interests. The seriousness of the effects that protecting copyright has on the privacy interests of users is significant: the fact that a tracing mechanism makes use of a systematic record which details what multimedia files are downloaded through a specific IP address, history of files shared or downloaded, or a list of the peers with whom a user has interacted in the past, ultimately disrespects the private space of the user [Hamlen and Thuraisingham, 2007]. Moreover, within P2P distribution systems, a collection of identifiable personal data should be limited to the minimum since anonymity is one of the basic functions of privacy. In these systems, anonymity is mainly concerned with protecting the identity of the end users as well as communication among users [Ding et al., 2003].

There is an inherent conflict of interest between copyright protection supporters and privacy advocates. There is a need to balance security and privacy needs when developing P2P content distribution systems. P2P developers should design these systems in a way that could satisfy both providers and receivers: content providers should not be reluctant to distribute their contents to a large number of people without the fear of copyright violation and simultaneously, enable end users to receive legal and malicious-free content without fear of privacy breach. Moreover, these systems should provide a tracing mechanism to trace the original uploader of any content in the system. Currently, this is a hot research area among researchers who are focusing on preservation of content providers ownership properties and content receivers' privacy and anonymity. Cryptographic and fingerprinting mechanisms [Megías and Domingo-Ferrer, 2013; Domingo-Ferrer and Megías, 2013; Li et al., 2010] are utilized to distribute contents within P2P systems such that the content provider neither knows the receiver's copy nor his identity. Only on finding an illegally re-distributed copy, the content provider identifies the re-distributor, thus promoting conditional privacy.

Intuitively, there is large scale of interdependence amongst security, privacy and anonymity aspects within P2P content distribution systems, thus favoring the combined approach taken in this study. This paper surveys current P2P distribution systems in terms of technological aspects of security, privacy and anonymity, aiming to provide a comprehensive account of the implemented mechanisms and their features.

The remainder of this paper is a survey of research in these areas. In Section 1, we discuss the challenges being faced by P2P developers in building secure and anonymous P2P systems. Section 2 briefly gives an overview of implemented

mechanisms and frameworks. In Section 3, we discuss the open problems of implemented systems and finally we present the conclusions of the survey in Section 4.

1. Security, privacy and anonymity challenges in legal P2P content distribution systems

P2P systems possess inherent challenges in terms of security, privacy and anonymity because of its loose peer management and extremely distributed working principles. Hence, devising security, privacy and anonymity protection mechanisms for P2P systems poses challenges for researchers and software engineers. According to Balfe et al. [Balfe et al., 2004] and Wasef and Shen [Wasef and Shen, 2009], the main challenge in creating P2P systems stems from the perceived need of providing anonymity for users of the system and the growing need of offering robust access control, confidentiality and data integrity. Illegitimate attacks in which malevolent parties may assume multiple identities undermine the efficiency of P2P systems, and characterize a fundamental security threat [Piscitello, 2002]. This is because formulating essential security services is challenging in the absence of stable and verifiable identities [Ren et al., 2011].

The concepts of security, privacy and anonymity used in this paper are defined in the context of providing a legal content distribution in a P2P system, and are described as follows:

1. *Security:* A mechanism aimed to protect an intellectual property and provide trustworthiness.
2. *Privacy:* The protection of user-related information in such a way that no personal information of an end user is revealed, unless a user is found to be guilty of illegal re-distribution. It is also called a conditional privacy.
3. *Anonymity:* A method to protect the identity of provider and receiever and also to protect the contents of transferred data between them.

1.1. Security issues in P2P

Xiaosong and Kai [Xiaosong and Kai, 2009] and Brinkmeier et al. [Brinkmeier et al., 2009] studies highlight that the security state for P2P systems is worse unlike Client-Server system in which illegal or unauthorized data access can be prevented by a

IN3 Working Paper Series is a monograph series promoted by the Internet Interdisciplinary Institute (IN3) of the UOC
IN3 Working Paper Series (2013) | ISSN 2013-8644 | http://in3-working-paper-series.uoc.edu

central authority (server) which provides level of access to the clients (users), monitors and maintain logs of all the data requests and transfers made by these authorized users. In contrast to Client-Server system, P2P systems are not considered secure because of the absence of a centralized authority that can vouch for security parameters. According to Fan et al. [Fan et al., 2012], the diverse nature of the multimedia material presents a severe challenge to the establishment of effective strategies that would foster secure systems.

P2P networking renders multimedia distribution channels vulnerable to various forms of attacks, e.g., potential of being involved with copyright infringement, the possibilities of downloading files infected with malicious codes (affecting data integrity) and susceptibility to attacks [Lipinski and Macalpine]. The security requirements of P2P content distribution systems cover mainly four aspects: copyright protection, data confidentiality, integrity and trust. These aspects are described as follows:

1. *Data confidentiality:* Confidentiality refers to limiting information access and disclosure to authorized users only.
2. *Integrity:* Data integrity implies that the data transferred between requesting and providing peer is an exact copy of an original version, i.e. the transferred data has not been corrupted during transmission between peers due to accidental or malicious altering.
3. *Copyright protection:* It guarantees that no additional replication is allowed other than the permitted copies.
4. *Trust:* Trust in P2P systems is a peer's belief in another peer's identity and reliability based on reputation.

In a P2P context, these characteristics become significantly more challenging than in the case of traditional domains (Client-Server system) due to lack of centralized control, and distributive ownership. Robels et al. [Robels et al., 2009] studies draw attention to the prosecution of P2P users for sharing pirated software or re-distribution of copyrighted material. For example, the Recording Industry Association of America (RIAA) has filed suits against more than 20,000 individuals in U.S. using P2P content distribution systems.

Apart from being a source for pirated content, P2P content distribution systems share files that pose severe security risks to end users. With millions of connected users and even more available files, there is no way to verify the legitimacy and safety of shared files. The downloadable files could contain malicious codes that can attack users′ computer with worms, malware, viruses and more. For example, a severe virus known as Antinny, affected the Japanese-based P2P content distribution system Winny. This virus led to the disclosure of a large amount of U.S. military base security codes along with private documents of a police investigator [Ingram, 2006].

1.2. Privacy issues in P2P

Privacy is largely an access control issue. Legal or procedural approaches are insufficient, because they can easily be circumvented or changed. Proper solutions therefore, need to be developed at the architectural level, using techniques for revocable privacy. There is a need to design systems in such a way that no personal information of end users is revealed, unless a user violates the terms of service. Only in that case, his or her personal details and how he or she violated the terms would be revealed to the relevant authorities. Moreover, only the identity of a copyright violator should be revealed without affecting other innocent users of the system.

Many existing P2P content distribution systems with copyright protection mechanisms monitor activities of the users, i.e., what kind of data users are downloading, though which IP address they are using the service and with whom they are communicating. These systems are more concerned about security of multimedia data rather than protection of user privacy. Few P2P systems have been proposed that address both security concerns of providers and users' privacy concerns [Megías and Domingo-Ferrer, 2013; Domingo-Ferrer and Megías, 2013; Yen et al., 2013]

Cryptography, Digital Rights Management (DRM), and watermarking are digital content protection techniques against piracy. The hidden information, watermark, is used for copyright protection, tamper detection, covert communication, source tracking of leakage, and so forth. Two significant issues in these schemes need to be considered, i.e., the provider's security as well as the privacy of an end user. The demand to protect privacy information of end users is increasing along with the rise of privacy leakage. Thus, a privacy-secure content distribution mechanism needs to be integrated into P2P systems to facilitate both providers and users.

1.3. Anonymity issues in P2P

Anonymity is an important factor to account for in P2P content distribution systems. It can enable privacy protection and censorship resistance. The major anonymity issue within these systems is that the end users' identities and actions can be revealed by other users. To provide anonymity to users in these systems, the personal, private, and sensitive information, such as the user name, user identification and IP address of the user, must be hidden during communication with others.

From the P2P content distribution system's perspective, there exist three types of anonymity.

1. *Receiver Anonymity:* P2P sharing system with receiver anonymity hides the identity of the receiver.

2. *Provider Anonymity:* P2P sharing system with provider anonymity hides the identity of the provider.
3. *Mutual Anonymity:* P2P sharing system with mutual anonymity hides the identities of both receiver and provider from each other and also hides the comunication between these two entities.

Grodzinsky and Tavani [Grodzinsky and Tavani, 2005] highlight the absence of anonymity in P2P systems by noting that the user reveals his or her details, such as plain-text queries and IP addresses, to another user (provider) that provides the services when downloading files. Furthermore, Walkowiak and Przewoźniczek [Walkowiak and Przewoźniczek, 2011] and Wang et al. [Wang et al., 2011] highlight that a great deal of information regarding the user preferences can be collected in video distribution by tracking the user activities at the provider side, thus compromising the user's anonymity. For example, in 2009, it was discovered through P2P sharing system, that an IP address in Iran had obtained blueprints and the avionics package for Marine One (the U.S.'s president's helicopter) [Mack, 2009].

The conflict between privacy and security within P2P content distribution systems manifests itself in a debate between anonymity and accountability, i.e. decreased anonymity (less user privacy) is proportional to increased accountability (more security to provider). However, both accountability and anonymity properties must exist side-by-side within these P2P systems. Various accountable anonymity mechanisms [Xu et al., 2012] have been proposed by researchers in which users enjoy anonymity under typical conditions and only those users get revoked who are found guilty of illegal re-distribution.

Similarly, the open nature of P2P systems makes data privacy a major challenge. Since in P2P system, there is no central authority that can authenticate and protect against malicious end users, it is up to the user to protect it and be responsible for its own actions. Consequently, each user in the system needs to evaluate the information received from another user in order to determine the trustworthiness about the information as well as the provider. This can be achieved by employing trust management techniques [Ding et al., 2008] within these systems. However, most trust models in P2P systems are identity-based; hence there exists a trade-off between trust and anonymity. Mechanisms should be devised such that real identities of end users are protected during authentication.

2. Mechanisms to counter challenges in P2P content distribution systems

This section discusses implemented mechanisms that strive to overcome security, privacy and anonymity issues in P2P content distribution systems.

2.1. Mechanisms for security

Various researchers have devised techniques and mechanisms to address security properties. Following are some mechanisms that are being utilized by companies and P2P developers to protect digital copyrights.

2.1.1. Encryption

Encryption is a core technique for content protection which provides data confidentiality and integrity. Before distribution, the content is encrypted by the content provider and the decryption key is provided only to those users who have permission to access the legitimate copies of the content. The encrypted content is useless to a pirate without an appropriate key [Grangetto et al., 2006]. Despite the fact that such techniques can protect the multimedia contents during their transmission, they cannot prevent a user from re-distributing the data illegally once they have been received and decrypted. However, this problem can be solved by establishing a Digital Rights Management (DRM) capability.

2.1.2 Digital Rights Management

DRM is a technology that is used to provide data confidentiality, i.e., it prohibits illegal copy and distribution of digital contents and permits only authorized users to access the contents. These systems were originally intended to help content providers in secure distribution of digital media to a large number of users in a manner that protects the interests of the owner only.

DRM architectures can be divided in three areas: content creation, content management and content usage. Content creation includes the creation of the media content and defining the rights. Content management is about content distribution and trading of the rights. Finally, content usage is used to enforce that rights are adhered to and to track content usage. However, there are few DRM solutions in P2P networks.

IN3 Working Paper Series is a monograph series promoted by the Internet Interdisciplinary Institute (IN3) of the UOC
IN3 Working Paper Series (2013) | ISSN 2013-8644 | http://in3-working-paper-series.uoc.edu

Kalker et al. [Kalker et al., 2004] describe a solution based on DRM for the problem of copyright infringement in P2P networks for music sharing. Li et al. in [Li et al., 2010] have proposed a DRM enabled P2P architecture which provides secure distribution of copyright-protected music contents and efficient tracing of unauthorized users. Chen et al. proposed a DRM mechanism in [Chen et al., 2009] for a BitTorrent like P2P system which provides end-to-end content secrecy and access control.

To copyright holders, P2P distribution systems are the main source of copyright infringement and DRM is the only way to prevent the content distribution systems from damaging the media industry. However, to the end users of a DRM-enabled P2P distribution system, DRM represents the media industry's attempts at playing "Big Brother", monitoring and controlling users' behaviors in ways that are inconsistent with their privacy interests. Thus, content providers need to work out with P2P developers how they can integrate DRM functionality with P2P systems so that they can offer their users P2P functionality while also protecting themselves from copyright abuse.

2.1.3 Digital Watermarking

Watermarking based on steganographic systems embed information directly into multimedia contents. It is recognized as a promising technique developed to address the problems of copyright protection, content integrity, tamper detection etc. There are two forms of watermarking, copyright watermarking and fingerprint watermarking (fingerprinting).

- In copyright watermarking, a copyright message (watermark) is embedded into the content which indicates copyright holder's identification. This is used to declare the copyright and cannot be used to trace the copyright violator.
- In fingerprint watermarking (fingerprinting), a user specific identification mark is embedded into content so that it can be used to track an illegal re-distributor.

Digital watermarking has become a significant area of research and development, and the usage of these techniques is now being considered a requisite to address the issues faced by the proliferation of digital content. Watermarking schemes have some important desirable properties (e.g. robustness, imperceptibility and capacity) and each of these properties must be taken into consideration when applying a certain watermarking technique.

1. *Robustness:* Robustness against attacks is a key requirement for watermarking. Watermarks must be robust enough to withstand all kinds of signal processing operations (at least below some distortion threshold), attacks or unauthorized access.
2. *Imperceptibility:* A watermark must be embedded into the content such that no obvious difference in the content fidelity can be noticed.

3. *Capacity:* It refers to the maximal data volumes that can be embedded into a multimedia content. The amount of information that can be embedded in a watermarked content is called data payload.

However, these essential watermarking properties contradict one another, i.e. if one is increased, the other decreases. For example, if a watermark capacity is increased, it affects the fidelity (perceptual similarity) of the content and if the watermark payload (capacity) is decreased, the robustness of the system is usually increased. Thus, it is very important for researchers to achieve a convenient trade-off between the above mentioned properties according to the application requirements. Various watermarking schemes [Fallahpour and Megías, 2011; Cao and Huang, 2012] have been proposed to achieve a better trade-off between these properties.

Digital watermarking can be used to in P2P content distribution systems to provide benefits to both content providers and end users. Velastin and Lian [Velastin and Lian, 2010] assert that the content distribution based on watermarking would foster security in P2P content distribution systems. Tsolis et al. [Tsolis et al., 2011] have proposed a P2P sharing system which not only allows digital content exchange but also supports copyright protection and management through watermarking technologies.

The other form of watermarking, i.e., digital fingerprinting, is used to uniquely identify the person responsible for illegal re-distribution. Once an unauthorized copy is found, the embedded fingerprint can uniquely identify the copyright violator. Literature review shows that there has not been much research work done related to fingerprinting protocol design for P2P applications. [Megías and Domingo-Ferrer, 2013; Domingo-Ferrer and Megías, 2013; Li et al., 2010] signify few of the work being done related to fingerprint watermarking in P2P content distribution systems.

2.1.4 Trust Management

P2P content distribution systems have become a major source for the spread of malware. Little efforts have been done to prevent malware spread within these systems. To prevent malware spread in these systems, reputation-based trust mechanisms can be used to find the reputed users to exchange with, or to avoid malicious nodes [Zhang et al., 2008]. Reputation-based trust systems have been considered by many researchers to mitigate the undesired behavior of malicious entities in P2P systems. By using reputation method, the system can provide users with a record of other peer's transactions. This will give the peer an indication about who should they trust before interacting with that peer.

Ding et al. have proposed a model based on trust management scheme that can mitigate the malware proliferation in P2P content distribution systems [Ding et al., 2008]. Zhou et al. in [Zhou et al., 2005] investigated the worms taking advantage of

P2P weakness and proposed several countermeasures based on individual P2P users to carry out detection and post-detection mitigation.

Trust management is challenging in P2P systems because a peer does not know all the other peers in the system. As a result, an efficient trust management model is needed to manage and distribute the trust on peers in order to make the difference between honest and malicious peers.

2.2. Mechanisms for privacy

Privacy in P2P content distribution systems with copyright protection can be granted using techniques such as anonymous fingerprinting and DRM with privacy.

2.2.1. Anonymous fingerprinting

In the aforementioned fingerprinting type, the goal is to protect content providers against illegal re-distributors. However, to protect user's privacy from content providers, another type of fingerprinting, i.e., anonymous fingerprinting [Chang et al., 2010] is used. This technology preserves users' rights for privacy by providing anonymity and the unlinkability of their P2P activity. However, there is significantly lesser research work done on privacy preserving mechanisms in P2P systems with legal content distribution.

Megías and Domingo-Ferrer [Megías and Domingo-Ferrer, 2013] have proposed a novel concept of automatic fingerprint recombination designed for P2P content distribution systems. The proposed scheme utilizes the fingerprinting concept to provide identification to the copyright owner and detect illegal digital content re-distributors. Furthermore, the users can preserve their privacy as long as they do not get involved in illegal content re-distribution. In [Domingo-Ferrer and Megías, 2013], Domingo-Ferrer and Megías have proposed a P2P protocol for distributed multicast of fingerprinted content. In the proposed framework, cryptographic primitives and a robust watermarking technique have been utilized to produce different marked copies of the content for the requesting user such that it can help the provider to trace re-distributors without affecting the privacy of honest users.

There is a need to develop such fingerprinting protocols for P2P content distribution systems that can help against copyright infringement and protects the privacy of innocent and honest users. Efficient traitor-tracing algorithms must be developed to prevent privacy breach of honest users.

2.2.2 DRM with privacy

Most of proposed DRM mechanisms focus on the protection mechanisms for digital contents and pay less attention to the users' privacy rights. In literature, only a few DRM mechanisms in P2P can be found, which address both content provider security and end user privacy. In [Sun et al., 2009], Sun et al. proposed an identity-based DRM system with privacy enhancement. Their DRM system retains user privacy by hiding the relationship information between users and the digital contents the users own.

2.3. Mechanisms for anonymity

Various P2P anonymous mechanisms have been proposed and implemented, aiming to provide protection to end users and middle nodes within the system.

2.3.1. Anonymous communication

Onion routing [Syverson et al., 2000] is a distributed P2P mechanism that allows two users to communicate anonymously over the network. It protects its communication against traffic analysis. The main aim of onion routing is to prevent intermediary nodes from knowing the source, destination and contents of the message. Onion Routing has been adapted in several anonymous P2P systems such as Anonymous P2P File Sharing (APFS) [Scarlata et al., 2001] or Tor [Dingledine et al., 2004], to provide anonymous communication between users.

Yu et al. [Yu et al., 2011] have proposed a P2P protocol, Nemor, which not only allows a requesting user and a serving user (provider) to communicate anonymously with each other and from other participating users, but also protects the identity of the content being exchanged. Another P2P protocol, Peer-to-Peer Personal Privacy Protocol (P5) [Sherwood et al., 2002], uses a hierarchical broadcasting technique to achieve mutual anonymity between users. For different levels of the hierarchy, different levels of anonymity are provided.

However, in order to achieve anonymity in P2P systems, there is a performance overhead due to encryptions and decryptions, insertion of fake traffic and an increased routing path to provide anonymity between two communicating users. P2P developers need to achieve an efficient trade-off between anonymity and efficiency to enable end users to use these systems without much delay.

2.3.2 Anonymous Authentication

It is impractical to pursue user anonymity without taking accountability into consideration. Accountability has traditionally been achieved through authentication mechanisms, which verify the identity of a user who requests a service. In order to preserve anonymity within these accountable systems, trust mechanisms are utilized, e.g. in [Lu et al., 2007], the protocol proposed by Lu et al. uses an anonymous zero-knowledge authentication protocol to support trust management such that users can use unforgeable and verifiable pseudonyms instead of their real identities. Similarly, Wang et al. in [Wang et al., 2010] have proposed an anonymous collaboration signature authentication protocol in which each user, instead of using his or her real identity, owns an un-forgeable and verifiable identity signature and this identity signature is signed by a trusted party through a collaboration signature method.

In P2P systems with anonymous authentication, if the privacy of peers is increased, the difficulties of ensuring authenticity and security are increased too. There is a clear trade-off between authentication and anonymity that is to be catered by P2P distribution system developers. Also the use of trusted party for authentication can be risky. Thus there is a trade-off between accountability and trusted party for authentication.

Table I gives a comparison of the presented P2P systems with respect to security, privacy and anonymity properties.

Table 1: Comparison of implemented P2P Systems with respect to security, privacy and anonymity

P2P Systems	Guaranteed Properties		
	Security	Privacy	Anonymity
A novel DRM framework for P2P music content delivery (Li et al.) [Li et al., 2010]	Data confidentiality and data Integrity through DRM and Encryption	No	No
Decentralized digital content exchange and copyright protection (Tsolis et al.) [Tsolis et al., 2011]	Copyright protection through Digital Watermarking	No	No
A Dynamic Trust	Trust through	No	No

IN3 Working Paper Series is a monograph series promoted by the Internet Interdisciplinary Institute (IN3) of the UOC
IN3 Working Paper Series (2013) | ISSN 2013-8644 | http://in3-working-paper-series.uoc.edu

Management Scheme to Mitigate Malware Proliferation in P2P networks (Ding et al.) [Ding et al., 2008]	Reputation-Based Trust mechanism		
Privacy-aware peer to peer content distribution using automatically recombined fingerprints (D. Megías and J. Domino-Ferrer) [Megías and Domingo-Ferrer, 2013]	Data integrity and copyright protection through Encryption and Digital Fingerprinting	Conditional Privacy through fingerprinting	Mutual Anonymity through Anonymous Communication
Distributed Multicast of Fingerprinted Content Based On a Rational P2P Community (J. Domingo- Ferrer and D. Megías) [Domingo-Ferrer and Megías, 2013]	Data integrity and copyright protection through Encryption and Digital Fingerprinting	Conditional Privacy through Digital Fingerprinting	Anonymous Communication
A ticket based digital rights management model (Sun et al.) [Sun et al., 2009]	Data confidentiality and Integrity through DRM and Encryption	Conditional Privacy through DRM	No
Nemor: A congestion-aware protocol for anonymous peer-based content distribution (Yu et al.) [Yu et al., 2011]	No	No	Mutual Anonymity through Anonymous Communication
P2P protocol Peer-to-Peer Personal Privacy Protocol (P5)	No	No	Mutual Anonymity through Anonymous Communication

(SHERWOOD ET AL.) [SHERWOOD ET AL., 2002]			
PSEUDO TRUST: ZERO-KNOWLEDGE AUTHENTICATION IN ANONYMOUS P2PS (LU ET AL.) [LU ET AL., 2007]	DATA INTEGRITY AND TRUST THROUGH ENCRYPTION AND TRUST-BASED MECHANISM	NO	MUTUAL ANONYMITY THROUGH ANONYMOUS AUTHENTICATION

3. Open problems in implemented mechanisms

The field of P2P technology presents a number of interesting challenges which include new methods for providing security, privacy, reliability and anonymity. Section II gives an overview of P2P mechanisms which have been defined and implemented by various researchers and software developers to address one or all of the above mentioned challenges.

Using P2P systems for distributing content is challenging due to the lack of a central authority. Considerable amount of research work has been carried out by researchers to provide an appropriate balance between distributing content on a large-scale and preserving the right of copyright owners. Much of the work has been done by using applications of watermarking, fingerprinting and DRM mechanisms.

Most of the research work involving fingerprinting protocols for copyright protection incurs high computational and communicational burdens due to the use of public-key encryption of the contents, secure multiparty protocols, zero-knowledge proofs and other techniques. Also, research work for developing robust and secure watermarking schemes is still in progress. The trade-offs between robustness, capacity and imperceptibility of watermarking schemes are yet to be achieved. Also, there is a need to develop an efficient traitor tracing scheme, such that the anonymity of honest users is preserved. Similarly, the proposed works on DRM mechanisms in P2P systems have not been able to effectively prevent copyright infringement and privacy breach of end users.

It is worth noting that, in achieving anonymity in P2P systems, there is a performance overhead. Much effort has been devoted to improve the performance of anonymous communication systems by working on resource localization, overlay

IN3 Working Paper Series is a monograph series promoted by the Internet Interdisciplinary Institute (IN3) of the UOC
IN3 Working Paper Series (2013) | ISSN 2013-8644 | http://in3-working-paper-series.uoc.edu

topology, path construction and encryption/decryption schemes. Therefore, better anonymity and efficiency tradeoffs are of primary importance for these systems to be deployed and gain user acceptance.

Another challenge faced by these systems is the harmonization between anonymity and accountability. There is a need to devise security mechanisms to ensure anonymity for honest users and traceability for misbehaving users in P2P systems. Similarly, another problem is that the users of these systems require anonymity but the government, media and software industry want some monitoring tools to be incorporated within the software in order to track illegal re-distributors. Thus, there is a need to balance the anonymity of users and security of copyright holders.

4. Conclusions

This survey illustrates that P2P systems face serious challenges in terms of combining security, privacy and anonymity. It is apparent that privacy, security and anonymity in P2P networks need critical attention in order to improve the efficiency of these systems. Efforts in addressing these concerns are still unsuccessful because of the intricacy of each other. Often, exertion for addressing one of these factors may increases the severity of the other, i.e. the review has indicated that strategies with the intention of enhancing privacy and anonymity in P2P systems are often characterized with serious security concerns and vice versa. Consequently, strategic solutions for addressing security issues in P2P networks should be sensitive to ideas of privacy and anonymity.

Although P2P systems are deployed and used on a large scale, there remain many open issues as discussed above that need to be addressed by researchers and P2P developers.

Acknowledgment

This work was partly funded by the Spanish Government through projects TSI2007-65406-C03-03 ‘‘E-AEGIS’’, TIN2011-27076-C03-02 ‘‘CO-PRIVACY’’ and CONSOLIDER INGENIO 2010 CSD2007-0004 ‘‘ARES’’.

References

Balfe S.; Lakhani A.D.; Paterson K.G. (2004) "Trusted computing: providing security for peer-to peer networks*", In of Proc. Fifth IEEE International conference on Peer-to-Peer Computing*, pp. 117-124.

BitTorrent (2001), "BitTorrent Homepage", http://www.bittorrent.com/ [Date of query:June 12, 2013]

Brinkmeier M.M.; Fischer M.; Grau S.; Schäfer G.; Strufe T. (2009) "Methods for improving resilience in communication networks and P2P overlays", *PIK - Praxis DerInformationsverarbeitung Und Kommunikation*, vol. 32, pp. 64-78.

Cao J.; Huang J. (2012) " Controllable secure watermarking technique for trade off between robustness and security", *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 821-826.

Chang C.-C.; Tsai H.-C.; Hsieh Y.-P. (2010) "An efficient and fair buyer-seller fingerprinting scheme for large scale networks", Computers & Security, vol. 29, no. 2, pp. 269-277.

Chen Y.Y.; Jan J.K.; Chi Y.Y; Tsai M.L. (2009) "A feasible DRM mechanism for BT-like P2P system", *In Proc. of Int. Symp. on Information Engineering and Electronic Commerce*, pp. 323–327.

Deewan P.; Daasgupta P. (2010) "P2P reputation management using distributed identities and decentralized recommendation chains", *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, pp. 1000-1013.

Ding C.H.; Nutanong S.; Buyya R. (2003) "Peer-to-Peer networks for content sharing", GRIDS-TR-2003-7, Grid Computing and Distributed Systems Laboratory, University of Melbourne, Australia, Tech. Report.

Ding X.; Yu W.; Pan Y. (2008) "A dynamic trust management scheme to mitigate malware proliferation in P2P Networks", *In Proc. of IEEE International Conference on Communications*, pp. 19-23.

Dingledine R.; Mathewson N.; Syverson P. (2004) "Tor: The second- generation onion router," *In Proc. of the 13th USENIX Security Symposium*, vol. 13, pp.303- 320.

Domingo-Ferrer J.; Megías D. (2013) "Distributed multicast of fingerprinted content based on a rational peer-to-peer community", *Computer Communications*, vol. 36, pp. 542-550.

eDonkey2000 (2000), "edonkey Project Homepage", http://*www.emule-project.net/* [Date of query: June 12,2013]

Fallahpour M.; Megías D. (2011) "High capacity audio watermarking using the high frequency band of the wavelet domain", *Multimedia Tools and Applications*, vol. 52,vol. 2-3, pp.485-498.

Fan X.; Li M.; Ma J.; Ren Y.; Zhao H.; Su Z. (2011) "Behavior-based reputation management in P2P file-sharing networks", *Journal of Computer & System Sciences*, vol. 78, pp. 1737-1750.

Grangetto M.; Magli E.; Olmo G. (2006) “Multimedia selective encryption by means of randomized arithmetic coding”, *In Proc. of IEEE Transactions on Multimedia*, vol. 8, no. 5, pp. 905-917.

Grodzinsky F.S.; Tavani H.T. (2005) “P2P networks and the verizon v. RIAA case: Implications for personal privacy and intellectual property”, *Ethics and Information Technology*, vol. 7, pp. 243-250.

gtk-Gnutella (2000), “gtk-Gnutella Homepage”,

http://gtk-gnutella.sourceforge.net/en/?page=news [Date of query: June 12, 2013]

Hamlen K.W.; Thuraisingham B. (2007) “Secure peer-to-peer networks for trusted collaboration”,in Proc. of International conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 58-63.

Ingram M. (2006) “66,000 Names and Personal Details Leak on P2P”, http://www.slyck.com/news.php?story=1169. [Date of query: June 10, 2013]

Kalker T.; Epema D.H.J.; Hartel P.H.; Lagendijk R.L.; Steen M-Van. (2004) “Music2Share-Copyright–compliant music sharing in P2P systems”, *In Proc.of IEEE special issue on Digital Right Management*, vol. 92, no. 6, pp. 961-970.

Li J.S.; Hsieh C-J.; Hung C-F. (2010) “A novel DRM framework for peer-to-peer music content delivery”, *J. Syst. Softw*, vol. 83, pp. 1689-1700.

Li X.; Krishnan S.; Ma N-W. (2010) "A wavelet-PCA-based fingerprinting scheme for peer-to-peer video file sharing", *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 365-373.

Lipinski B.; Macalpine P. “A security review of anonymous peer-to-peer file transfer protocol”, Technical Report, Rice University, Houston, TX, USA. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.2925 [Date of query: June 10, 2013]

Lu L.; Han J.; Liu Y.; Hu L.; Huai J.; Ni L.M.; Ma J. (2007) “Pseudo Trust: Zero-knowledge uuthentication in anonymous P2Ps”, *IEEE Transactions on Parallel and Distributed Systems*, pp. 1-10.

Mack M.B. (2009) “P2P survival guide:what users must know”, http://thehill.com/opinion/op-ed/8129-p2p-survival-guide-what-users-must-know [Date of query: June 12, 2013]

MediaFire (2006), “MediaFire”, http://www.mediafire.com/ [Date of query: August 2, 2013]

Megías D.; Domingo-Ferrer J. (2013) “Privacy-aware peer to peer content distribution using automatically recombined fingerprints”, *Multimedia Systems*, in press.

Opera (1996), “Opera browser-The alternative web browser”, http://www.opera.com/computer/ [Date of query: June 10, 2013]

Pando Networks (2004), “Pando Networks”, http://www.pandonetworks.com/p2p/ [Date of query: June 13, 2013]

Passarella A. (2012) “A survey on content-centric technologies for the current internet: CDN and P2P solutions”, *Computer Communications*, vol. 35, no. 1, pp. 1-32.

Piscitello D (2002) “Security and peer-to-peer applications”, *Business Communications Review*, vol. 32, pp. 45-51.

Ren Y.; Cheng F.; Peng Z.; Huang X.; Song W. (2011) “A privacy policy conflict detection method for multi-owner privacy data protection”, *Electronic Commerce Research*, vol. 11, pp. 103-121

Robles R.J.; Choi M.K.; Cho E.S. (2009) “A paradigm solution to P2P security issues”, *In Proc. of International e-Conference on Advanced Science and Technology (AST '09), IEEE Computer Society*, pp. 3-7.

Scarlata V.; Levine B.; Shields C. (2001) “Responder anonymity and anonymous peer-to-peer file sharing", *In Proc. of the ACM CCS*, pp.17-26.

Sherwood R.; Bhattacharjee B.; Srinivasan A. (2002) “P5: A Protocol for scalable anonymous communication”, *In Proc. of IEEE Symp. on Security and Privacy*, pp.58-70.

Singh A.; Gedik B.; Liu L. (2004) “Agyaat: Mutual anonymity over structured P2P networks”, *Internet Research*, vol. 16, pp. 189-212.

Sun M-K.; Laih C.S; Yen H.Y.; Kuo J.R. (2009) "A ticket based digital rights management model", *In Proc. of IEEE Consumer Communications and Networking Conference*, pp. 1-5.

Syverson P.; Tsudik G.; Reed M.; Landwehr C. (2000) “Towards an analysis of Onion Routing security”, *Designing Privacy Enhancing Technologies*, *LNCS*, pp. 96–114.

Theotokis S.A.; Spinellis D. (2004) “A survey of peer-to-peer content distribution technologies”, *ACM Comput. Surv*, vol. 36, pp. 335-371.

TransferBigFiles (2007), “TransferBigFiles”, http://www.transferbigfiles.com/ [Date of query: August 2, 2013]

Tsolis D.K.; Sioutas S.; Panaretos A.; Karydis I.; Oikonomou K. (2011) “Decentralized digital content exchange and copyright protection”, *In Proc. of IEEE Symp. Computers and Communications*, pp. 1056-1061.

Velastin S.; Lian S. (2010) “Special issue on multimedia analysis and security”, *Springer Science*, vol. 57, pp. 1-4.

Walkowiak K.; Przewozniczek M. (2011) “Modeling and optimization of survivable P2P multicasting”, *Computer Communications*, vol. 34, pp. 1410-1424.

Wang X.; Sun X.; Sun G.; Luo D. (2010) “CST: P2P anonymous authentication system based on collaboration signature”, *In Proc. of IEEE 5th International Conference on Furture Information Technology*, pp. 1-7.

Wang Y.; Nakao A.; Vasilakos A.V.; Ma J. (2011) “P2P soft security: On evolutionary dynamics of P2P incentive mechanism”, *Computer Communications*, vol. 34, pp. 241-249.

Wasef A.; Shen X.(2009) “REP: Location privacy for VANETs using random encryption periods”, *Mobile Networks and Applications*, vol. 15, pp. 172-185.

Wyzo- The Media Browser (2010), “Home Page ”, http://www.wyzo.com/ [Date of query: June 10, 2013]

Xiaosong L.;Kai H. (2009) “Collusive piracy prevention in P2P content delivery networks”, *IEEE Transactions on Computers*, vol. 57, pp. 970-983.

Xu G.; Aguilera L.; Guan Y. (2012) "Accountable Anonymity: A proxy re-encryption based anonymous communication system", *In Proc. of IEEE 18th International Conference on Parallel and Distributed Systems (ICPADS)*, pp.109-116.

Yen C-Y.; Liaw H.T.; Lo N.W. (2013) "Digital rights management system with user privacy, usage transparency, and superdistribution support", *International Journal of Communication Systems*, in press.

Yu F.; Gopalakrishan V.; Lee D.; Ramakrishnan K.K. (2011) “Nemor: A congestion-aware protocol for anonymous peer-based content distribution”, *In Proc. of IEEE Conference on P2P computing*, pp. 260-269.

Zhang Q.; Zhuo Y.; Gong Z. (2008) “A trust inspection model based on society behavior similarity rule in dynamic networks”, *In Proc. of IEEE International Conference on Computer Science and Software Engineering*, pp. 970–973.

Zhou L.D.; Zhang L.T.; Mcsherry F.; Immorlica N.; Costa M.; Chien S. (2005) “A first look at peer-to-peer worms: threats and defenses”, *In Proc. of International Workshop on Peer-To-Peer Systems (IPTPS)*, pp. 24-35.

Resumen

Las últimas décadas han sido testigo de un rápido desarrollo de nuevas estructuras de red, tales como los sistemas Peer-to-Peer (P2P). Estos sistemas presentan diversas ventajas que hacen que los usuarios prefieran su uso, como por ejemplo conseguir que los costes de funcionamiento sean muy pequeños de manera que el proveedor pueda distribuir el contenido original y, al mismo tiempo, permitir a los usuarios finales acceder a los datos en un tiempo reducido. Pero, por desgracia, los sistemas P2P de distribución de contenidos de hoy en día son muy criticados a causa de las re-distribuciones ilegales. Esta actividad ilícita no solo es preocupante para los proveedores de contenidos, sino también para los usuarios finales de estos sistemas. La aplicación de los mecanismos de protección de derechos de autor en los sistemas de distribución de contenidos P2P plantea graves amenazas a la privacidad, ya que se supervisan las actividades de los usuarios finales dentro de estos sistemas de manera que estos puedan tener que rendir cuentas en caso de que se produzca una violación de los derechos de autor. Varios investigadores han examinado los desafíos que caracterizan a estos sistemas desde diversos puntos de vista, proponiendo diferentes soluciones. En este trabajo se lleva a cabo un estudio de la bibliografía incluyendo diversos trabajos pertinentes sobre el tema, con la intención de describir los desafíos y soluciones asociados con la distribución de contenidos legales en sistemas P2P. Para nuestro conocimiento, esta es la primera vez que se lleva a cabo un análisis del estado del arte en redes P2P que combina aspectos de seguridad, privacidad y anonimato.

Palabras clave

Protección del copyright, seguridad, privacidad, anonimato, redes Peer-to-Peer

Resum

Les últimes dècades han estat testimoni d'un ràpid desenvolupament de noves estructures de xarxa, com ara els sistemes Peer-to-Peer (P2P). Aquests sistemes presenten diversos avantatges que fan que els usuaris en prefereixin l' ús, com per exemple aconseguir que els costos de funcionament siguin molt petits de manera que el proveïdor pugui distribuir el contingut original i, al mateix temps, permetre als usuaris finals accedir a les dades en un temps reduït. Però, malauradament, els sistemes P2P de distribució de continguts d'avui dia són molt criticats a causa de les re-distribucions il·legals. Aquesta activitat il·lícita no només és preocupant per als proveïdors de continguts, sinó també per als usuaris finals d'aquests sistemes. L'aplicació dels mecanismes de protecció de drets d'autor en els sistemes de distribució de continguts P2P planteja greus amenaces a la privadesa, ja que se supervisen les activitats dels usuaris finals dins d'aquests sistemes de manera que aquests puguin haver de rendir comptes en cas que es produeixi una violació dels drets d'autor. Diversos investigadors han examinat els desafiaments que caracteritzen aquests sistemes des de diversos punts de vista, proposant-ne diferents solucions. En aquest treball es duu a terme un estudi de la bibliografia incloent diversos treballs pertinents sobre el tema, amb la intenció de descriure els desafiaments i solucions associats amb la distribució de continguts legals en sistemes P2P. Per al nostre coneixement, aquesta és la primera vegada que es duu a terme una anàlisi de l'estat de l'art en xarxes P2P que combina aspectes de seguretat, privadesa i anonimat.

Paraules clau

Protecció de copyright, seguretat, privadesa, anonimat, xarxes Peer-to-Peer

Author Biographies

Amna Qureshi
aqureshi@uoc.edu
Doctoral program in Knowledge and Information Society
Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (Spain)

Amna Qureshi is a Ph.D. student in Knowledge and Information Society Doctoral program at IN3 and is carrying out her research under the direction of Dr. Helena Rifà-Pous and Dr. David Megías. She holds the degree of Computer Engineering from COMSATS University (Pakistan) and the master in Computer Engineering from Center of Advanced Studies in Engineering (CASE, Pakistan). Her research interests include multimedia security, privacy, anonymity and copyright protection in peer-to-peer networks.

Helena Rifà-Pous
hrifa@uoc.edu
Researcher at IN3
Universitat Oberta de Catalunya (Spain)

Helena Rifà-Pous is an Associate Professor at Estudis d'Informàtica, Multimèdia i Telecomunicació in the Open University of Catalonia (UOC). She holds a Ph.D. in Telecommunications Engineering from Universitat Politecnica de Catalunya. She is a researcher in K-ryptography and Information Security for Open Networks (KISON) research group at IN3 (UOC). Her research focuses on security in open networks (adhoc, cognitive radio networks, sensor, etc) and public-key infrastructure systems. She has published several journal and conference papers in wireless security and data hiding. She is also member of scientific committee of several journals and conferences.

David Megías Jiménez
dmegias@uoc.edu
Researcher at IN3
Universitat Oberta de Catalunya (Spain)

David Megías Jiménez is a Professor at Estudis d'Informàtica, Multimèdia i Telecomunicació in the Open University of Catalonia (UOC). He holds a Ph.D. in Computer Science from Universitat Autonoma de Barcelona. He is the head of K-ryptography and Information Security for Open Networks (KISON) research group at IN3 (UOC). His research interests include security, privacy and copyright protection schemes. He has published several journal and conference papers in watermarking area both for image and audio contents and has also taken part in international projects such as the FP6 European Network of Excellence in Cryptology-ECRYPT. Dr. Megías is also member of the scientific committee of several journals and conferences and has been member of the organizing committee of several international conferences.

IN3 Working Paper Series is a monograph series promoted by the Internet Interdisciplinary Institute (IN3) of the UOC
IN3 Working Paper Series (2013) | ISSN 2013-8644 | http://in3-working-paper-series.uoc.edu

IN3 Working Paper Series is a monograph series promoted by the Internet Interdisciplinary Institute (IN3) of the UOC
IN3 Working Paper Series (2013) | ISSN 2013-8644 | http://in3-working-paper-series.uoc.edu