Exploiting Multimedia Services in Mobile Social Networks from Security and Privacy Perspectives

Kuan Zhang, Xiaohui Liang, and Xuemin (Sherman) Shen, University of Waterloo
Rongxing Lu, Nanyang Technological University

ABSTRACT

With the ever-increasing demands of multimedia services and the boom of smartphones, traditional online multimedia applications are extended to mobile users anywhere and anytime. However, the flourishing of multimedia services is still hindered by inherent security and privacy concerns. In this article, we investigate the security and privacy issues of multimedia services by studying a newly emerging multimedia-oriented mobile social network (MMSN), which helps users receive multimedia services not only from their online social communities but also from their social friends in the vicinity. Specifically, we first define the MMSN architecture, and identify the unique security and privacy challenges. Then we study three MMSN applications: content query, service evaluation, and content filtering. For each application, we present the specific security and privacy problems with the corresponding countermeasures. Finally, we propose some future research directions in the MMSN.

INTRODUCTION

Multimedia is progressively becoming content-driven and object-oriented, promoting applications with user collaboration in the current fashion. In 2012, in every minute of the day, 100,000 tweets are posted; 48 hours of videos are updated on Youtube with 2,800,000 video views; 685,000 pieces of contents are shared on Facebook; and 2,000,000 queries are conducted on Google. As the amount of multimedia services skyrockets, it is of paramount importance for users to not only share multimedia contents with each other but also receive the content of their interests. To this end, a ubiquitous and omnipotent platform for multimedia services is highly desired to meet the increasing user requirements.

A mobile social network fueled with heterogeneous wireless infrastructures (e.g., cellular/WiFi) and mobile devices (e.g., smartphones, tablets), has become a promising and popular platform to enable user collaboration and information sharing. It can also facilitate multimedia services by providing ubiquitous connections between service providers and users in a mobile environment. Such an integration of multimedia services and the mobile social network is dramatically changing users' lifestyles, and fosters a value-added research area of the multimedia-oriented mobile social network (MMSN).

This newly emerging MMSN provides users with up-to-date contents from a centralized server and local contents directly shared by their friends nearby [1]. Specifically, users can directly select and download the multimedia contents in which they are interested from centralized servers via the Internet; local service providers such as stores could disseminate local contents to mobile users in a distributed manner [2, 3]; and a group of users in one social community might autonomously form an opportunistic network and share personalized contents via peer-to-peer communication.

Despite the promising features of multimedia services provided by the MMSN, there are many new challenges in the privacy and security aspects [4]. In an MMSN, personalized content query is a typical multimedia service, but it may disclose a user's personal information to service providers. For example, Google could record a user's queries and analyze his/her preferences. Moreover, when users visit social networking sites with "Facebook Like" buttons and press the button, they disclose their preferences and personal information, such as location and identity, to the public. Obviously, when users make little effort to protect their personal information, their privacy might easily be violated in these applications.

In addition, malicious users might forge some contents to cheat other users in the system. Furthermore, service evaluation is another multimedia application where users post their reviews or experiences about services they use. However, Sybil attackers could forge a large number of

0163-6804/14/$25.00 © 2014 IEEE

pseudonyms and gain a disproportionately negative influence. In other words, these attackers would either purposely generate positive comments on their own services or arbitrarily produce negative reviews on other quality services. Therefore, preserving privacy and resisting malicious attacks are critical research challenges that need to be addressed for an MMSN.

In this article, we define the MMSN architecture and identify some research issues related to privacy preservation, trust relationships, and malicious attacks. Furthermore, we present three emerging MMSN applications: personalized content query, service evaluation, and content filtering. We investigate the security and privacy problems in these applications, and present the corresponding countermeasures. Finally, we present some potential research directions and conclude the article.

MMSN Architecture

In this section, we present the heterogeneous MMSN architecture and identify the entities with different communication patterns. Then we categorize the MMSN into different domains.

MMSN Architecture

The MMSN, as shown in Fig. 1, is a virtual environment composed of mobile users in a local area, local servers, and centralized servers.

Multimedia — Multimedia contents are central to the MMSN, and vary in different applications. Generally, multimedia can be global content, such as online video, local content (e.g., local flyers and advertisements), and personal contents including personal status and images. It may be small (e.g., text contents) and large (e.g., video, movies), ranging from multiple forms of contents, such as photo galleries with both images and descriptions, to videos and even movies.

Mobile Users — Mobile users with smartphones can either directly connect to the Internet via cellular/WiFi networks or communicate with neighboring users in the vicinity via Bluetooth/near field communication (NFC) techniques. The communication patterns and modes are determined by environmental conditions and application requirements. When users are searching the Internet contents such as Youtube video, they might switch to Internet mode and directly access the target servers to obtain the desirable contents. Users in the vicinity can directly exchange their personal contents, including local information and other multimedia contents with each other via Bluetooth. Mobile users not only are the content owners but also aim to query or obtain contents from others. The multimedia contents of mobile users contain text (i.e., news, microblog), image, music, and video, as well as others.

Local Server — The local server (LS) can provide local services, such as advertisements and service evaluation of stores, to users in the vicinity. LSs are equipped with smartphones or dedicated mobile local gateways, which disseminate their service information to neighboring mobile users and collect user feedback or requests. The LS's communication devices are storage-rich and fueled by adequate power. The multimedia contents of LSs are basically about local information including service description, local introduction and tips, advertisements, and so on.

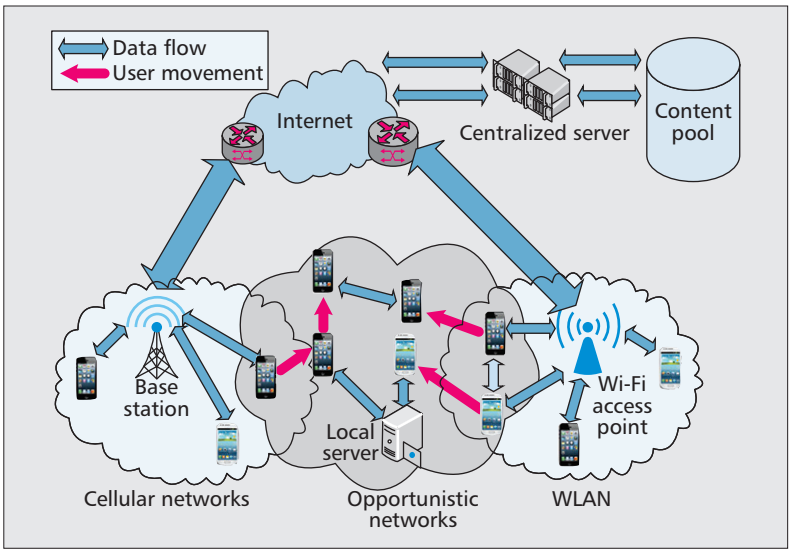

Figure 1. *Multimedia-oriented mobile social network.*

Centralized Servers — Centralized servers (CSs), such as Internet service providers and cloud servers, can provide centralized services to mobile users due to the high capabilities of storage, communication, and computation of CSs.

MMSN Domains

The MMSN can generally be divided into three domains: User-to-CS, User-to-LS, and User-to-User domains according to different communication patterns and multimedia contents as shown in Fig. 2.

User-to-CS Domain — In the User-to-CS domain, mobile users can directly connect with the CS via either cellular networks with a purchased mobile data plan or WiFi access points, which are pervasively deployed in the residential community and public spots such as campuses and stores. The communication range depends on the network infrastructures, and connections can be one-hop or multihop. The contents communicated within the User-to-CS domain contain a broad range of multimedia all over the world. Users can browse online multimedia contents, such as social media, photo galleries, and movies, query the desirable contents, and share their multimedia contents via the Internet.

User-to-LS Domain — In the User-to-LS domain, the LS acts as not only a temporary local server, which is equipped with the easy-to-setup and low-cost local wireless gateway or router, but also a mobile user who participates in the mobile user's social interactions. The LS may have the capability to access the Internet or establish the local distributed mobile social network among neighboring users. The LS can also

The contents in User-to-User domain are basically personal contents provided by users themselves. The goal is to share contents among users or social friends, or cooperatively complete some specific activities.

Figure 2. *Multimedia-oriented mobile social network domains: User-to-CS, User-to-LS, User-to-User.*

disseminate the contents to nearby mobile users with a longer communication range greater than that of the mobile user. The device that the LS takes is storage-rich and has a battery with plenty of power. Since the User-to-LS domain is featured by the local attribute, the LS provides multimedia services, local guidelines, and advertisements, and posts the local customer's reviews to make other customers better understand the properties of the store.

User-to-User Domain — When users are in a mobile environment where either continuous Internet services may not be guaranteed or users can directly exchange contents with each other in the vicinity, User-to-User communications plays an uppermost role. In a local area (i.e., shopping mall, commercial street), users with similar social preferences may want to share their multimedia contents with each other. They can utilize Bluetooth to establish a temporary connection for content sharing without the assistance of the Internet, where the communication range is from 1–100 m in the local area, and multihop communication is applied.

The contents in the User-to-User domain are basically personal contents provided by users themselves. The goal is to share contents among users or social friends, or cooperatively complete some specific activities.

Security and Privacy in MMSN

In this section, we identify the security and privacy challenges of the MMSN.

Privacy Disclosure

Since users are unwilling to disclose their own unique and private information including multimedia contents to others, especially strangers, privacy preservation is of paramount importance in an MMSN, where the contents may be highly relevant to users' privacy, such as identities, locations, preferences, and social relationships. Generally, cryptography is adopted to protect the contents from being directly eavesdropped by outside attackers when transmitting and processing [5]. Alternatively, an attribute-based access policy [6] could be utilized to confine other users' access capabilities. Li *et al.* [7] exploit secure profile matching to prevent users' unique and private information from being directly exposed to others when users are matching their profiles. Despite these cryptographic mechanisms, some private information disclosed to users' friends can still violate that user's privacy. When a user Bob queries some specific contents to the CS or his social friends, the query request might reflect Bob's preferences. Then the CS or other users might infer Bob's other attributes, violating his privacy. Sometimes, users are not even aware of the disclosure of their pri-

vacy, and do not intentionally protect themselves. Therefore, to achieve privacy can guarantee users a secure MMSN and provide a better multimedia service experience.

Trust Relationship

Trust is a typical feature of social-based applications in an MMSN, since the contents shared among social friends are more trustworthy than those from strangers [8]. Cutillo *et al.* [9] exploit trust relationships among users to facilitate the content sharing in a decentralized social network. In a mobile or local environment, to identify content authenticity and trustworthiness is still crucial since many delivered contents are from strangers instead of social friends. Particularly, in a local service evaluation [10], users may not fully trust reviews from strangers since a stranger's preferences could be quite different, and the reviews might not be useful. If the reviews can be related to the reviewer's preferences, the trustworthiness would be significantly improved. However, the linkability between the comments and the reviewer's preferences might disclose the reviewer's privacy. Privacy should also be preserved when exploring trust to improve the service experiences of users. The major challenge of trust in an MMSN is how to build trust relationships among mobile users and provide trustworthy contents to them.

Malicious Attacks

There may be malicious attackers in an MMSN who might launch attacks to either degrade network performance or violate legitimate users' information. In content sharing, a malicious user forges contents and shares fake ones with other users. In addition, during cooperation, malicious users might not contribute as much as other users pay or even launch denial of service attacks. Wang *et al.* [11] investigate users' long-term relations, including trust relationships, to facilitate content sharing and cooperation. Zhao *et al.* [12] propose a game theoretic framework to model and analyze colluding attackers in multimedia social networks. Particularly, in the service evaluation within the User-to-LS domain, an LS arbitrarily posts positive reviews and deletes negative ones, or colludes with some mobile users to forge comments. As a result, users cannot extract useful and correct information or review comments on target stores. In summary, security mechanisms should be adopted to resist malicious attacks and guarantee a secure MMSN for users.

Security Solutions for MMSN Applications

Content Query Application

Content query is a widely applied application in social networks and is an indispensable component of an MMSN. Indisputably, querying desirable contents reflects the user's ultimate mind and is an uppermost target in an MMSN. Content query could exist in User-to-CS, User-to-LS, and User-to-User domains according to the desirable content types. Since the CS not only has the largest capabilities of storage, computation, and communication, but also maintains the connections with worldwide content resources, contents from users could easily be pooled together on the CS side. With the connections (i.e., the Internet) to the CS, users usually directly submit their content query request containing their preferences. According to requests from users, CSs search the server and select the appropriate contents for users. With the recent advent of cloud computing, cloud servers represent the most highly engaged segment of content storage and processing, where cloud servers store the majority of the multimedia contents and process them, significantly saving the storage and computation consumption of the original servers.

Meanwhile, the security and privacy issues are not negligible, since the cloud server may not be fully trusted and might act as a malicious entity in an MMSN. First, a cloud server may be compromised by outside attackers. If all the contents are stored as the plaintext in the cloud server, content confidentiality would be violated. Several research efforts [6, 13] have been focused on the content confidentiality where the raw contents are encrypted and stored in the semi-trusted cloud servers. The key issue is how to efficiently store the massive number of contents and effectively process them as well. Second, during the content query, if a user queries some contents (encrypted and stored in the cloud servers) with some specific features, such as key words and some other properties, the cloud server cannot complete the query since the stored contents are in the ciphertext.

Under these circumstances, some research efforts [13, 14] have been made to address these issues in the User-to-CS domain. The hidden vector encryption (HVE)-based range query scheme [13] with privacy preservation can blind the query content in ciphertext so that the servers, including semi-trusted cloud servers, cannot directly learn the exact query of users but can compute the query result in the ciphertext. There are three phases: range query predicate construction, encrypted content upload, and range query, as shown in Fig. 3. The content owner u_o first chooses an index vector $\mathbf{x} = (x_1, \cdots, x_l)$ to symbol the content m, and encrypts m with the encryption key k_o. Meanwhile, k_o is encrypted under vector $\mathbf{x}$ with the CS's public key. Then the ciphertext of the content is sent to cloud server 1, while the ciphertext of k_o is sent to cloud server 2, where cloud servers 1 and 2 are independent entities. Then the query requester sets up the query token $\vec{\mathbf{w}}$ with the query translator component [14]. The requester then sends the query token to cloud server 2, where the query token and stored content index are cryptographically matched. Here, a predicate function over a set of binary strings Σ is $\mathcal{F}: \Sigma \rightarrow \{0, 1\}$, and $\mathcal{F}(X) = 1$ if and only if $X \in \Sigma$. A cryptographic function $Query(\mathbf{w},\mathbf{x}) = k_o$ if and only if $\mathcal{F}(\mathbf{w}) = 1$ (i.e., $\mathbf{w} \in \vec{\mathbf{x}}$). As a result, at cloud server 2, if the query token matches some index, the corresponding encryption key k_o could be selected and securely transmitted to the query requester. Finally, the query requester uses the index to obtain the ciphertext of content m from cloud server 1 and decrypts it with k_o. Since the token translator is automatically proceeded and

Privacy should also be preserved when exploring trust to improve the service experiences of users. The major challenge of trust in an MMSN is how to build trust relationships among mobile users and provide trustworthy contents to them.

In User-to-LS domain, there is no trusted authority to build up the trust relationships between users and LSs. How to provide the trust evaluation for the LS is crucial and would benefit both LSs and users.

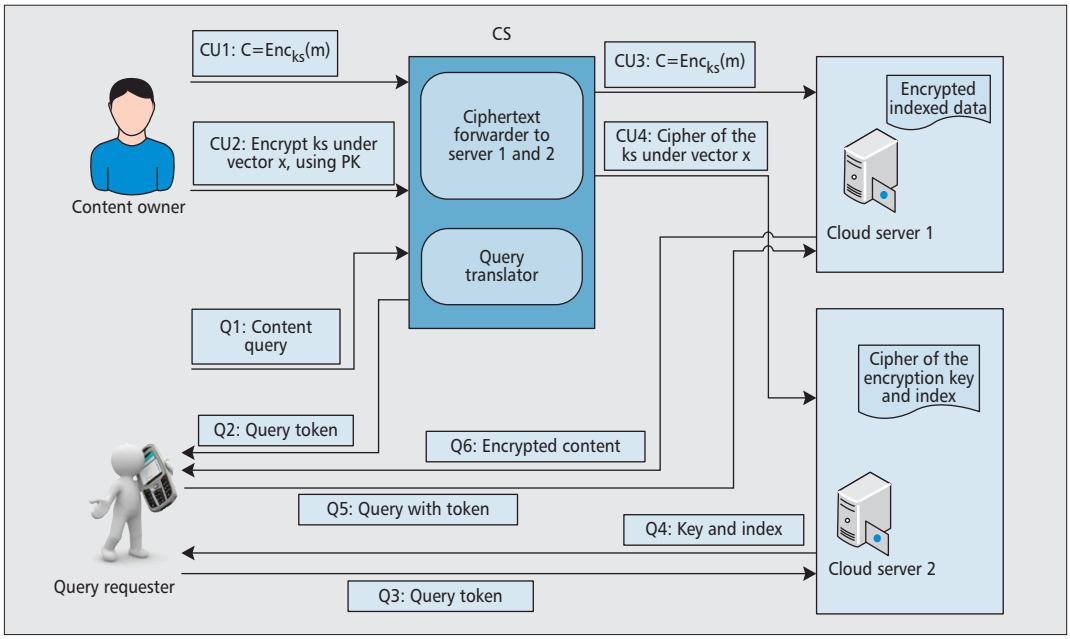

Figure 3. *Privacy-preserving range query in MMSN. CU denotes content uploading, and Q denotes query procedures.*

transparent to the CS, the query is not directly disclosed. After the query requester obtains the query token, the query content is hidden in the token. Therefore, the privacy of both content owner and query requester can be preserved.

Service Evaluation Application

Service evaluation is another attractive and value-added application in an MMSN. When users are in a shopping mall or on a commercial street, they might like to find features of local stores. One way is to search in web-based social networks, such as Facebook or eBay (a global online marketing tool), via the Internet to browse other customers' reviews. These online reviews are not as real-time as possible since customers might not instantly leave their reviews online. Furthermore, since not all customers provide their reviews, the posted reviews might not properly reflect the service quality of the local stores. An emerging approach is to enable the LS to directly collect all customers' reviews and make them public to local customers, which is driven by the demands of both LSs and users if the LSs would also diffuse their advertisements to local users to attract them. The challenging issue is how to convince users and make them trust the posted reviews, since the trust relationship among local mobile users would not be very strong. In the User-to-LS domain, there is no trusted authority to build up the trust relationships between users and LSs. How to provide trust evaluation for the LS is crucial, and would benefit both LSs and users. Furthermore, some malicious attackers might exist in the network and negatively impact the reviews. If the vendors become the attackers, they might forge some positive reviews, and delete or modify the negative ones. Furthermore, the attackers could submit fake review comments.

In [10], Liang *et al.* propose a trustworthy service evaluation system to enable users to share their review comments in service-oriented mobile social networks (in the User-to-LS domain). Several tokens are generated by the LS and then circulated among users to synchronize their review submission behaviors. If a user would like to leave a review, he/she completes the review submission until he/she receives a token from either the LS or other users who have similar preferences. Then this user either directly submits a review and returns the token to the LS, or cooperates with other neighboring users who also want to submit reviews to the same LS in order to submit an integrated review. The signature and aggregate authentication techniques are adopted to maintain review integrity and efficiently verify the users' signatures. A timestamp is added to the review signature so that no user can modify past reviews. The tokens generated by the LS can build an independent review chain. The LS maintains a token pseudonym list where each token is associated with a pseudonym that belongs to the user who most recently submitted a review with this token. When a new review is received, the list will be updated and periodically broadcast to all users in the communication range of the LS. After publishing a token, the LS cannot delete this token from the token pseudonym list even if a review is negative. The length of the review chain for every token determines the LS's modification capability; that is, the LS must have higher capability to modify the review chain if the length of the review chain is longer. In addition, the privacy-preserving profile matching technique [7] is utilized to help neighboring users find common preferences between them. These common preferences could facilitate them to establish a trust relationship.

In this application, Sybil attacks, where an attacker abuses pseudonyms to produce multiple unlinkable fake reviews in a short time, and review attacks, where attackers delete or modify reviews, can be resisted based on the specific

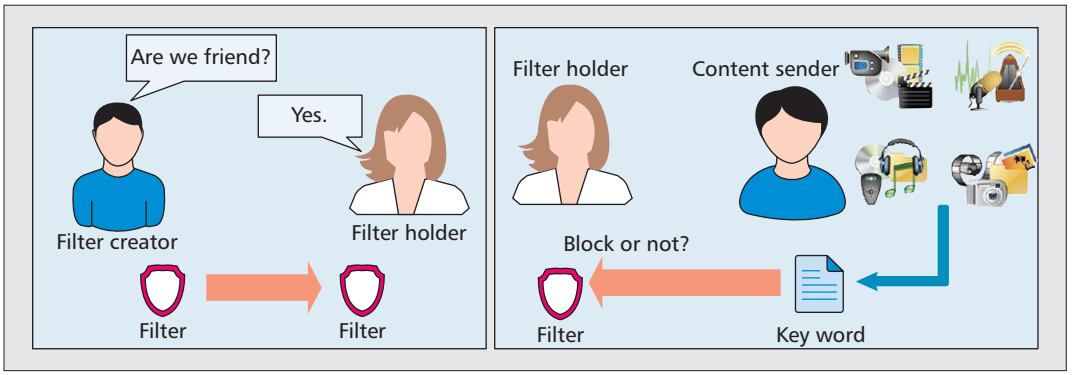

Figure 4. *Content filtering. The filter creator first distributes the filter to his friends. Then the filter holders help select the desirable multimedia contents for the filter creator.*

If a user produces a massive number of reviews with the same pseudonym in a time slot, this user can easily be detected by the public. Therefore, Sybil attacks can be effectively detected, and the malicious reviews are rejected.

token structure [10]. To resist Sybil attacks, the time window is divided into time slots. If a user produces a massive number of reviews with the same pseudonym in a time slot, this user can easily be detected by the public. Therefore, Sybil attacks can be effectively detected, and the malicious reviews are rejected.

Spam Content Filtering Application

In a shopping mall or local area, many service providers disseminate their advertisements and flyers to customers, especially in the User-to-LS and User-to-User domains. In such a case, users may want to receive interesting service information instead of useless spam contents, especially in a shopping mall or on commercial streets. For example, Bob is looking for the clearance jeans on a commercial street where he only requires the service contents about specific stores rather than restaurants or groceries. Intuitively, Bob could distribute some key-word-based filters containing his preferences to other users to block the unwanted contents and ensure the delivery of the useful ones. Thus, the selection of filter holders is of paramount importance in cooperative content filtering. In addition, during lunchtime, Bob may want contents about nearby Italian restaurants instead of the previous shopping strategy. Thus, quick update of the distributed filters is driven by user demands such that users can always receive the information they want. On the other hand, since the filters contain the key word contents that reflect the filter creator's preference, a user's privacy might be violated if directly distributing the filters to others. Therefore, protecting the user's key word contents from direct exposure to others is crucial.

In [15], Zhang *et al.* propose a social-based spam filtering scheme for mobile social networks and consider the distribution and update. Based on the investigation of social impacts, they devise a filter distribution mechanism where the filters are purposely sent to the filter creator u_i's social friends having several common attributes with u_i, as shown in Fig. 4. Since the social friends in a mobile environment would encounter u_i frequently, it is possible for the content senders to select them as the relay to disseminate the service contents to u_i. As a result, u_i's friends could block the spam contents in advance so that the network resources are extensively saved without useless or spam content delivery. Furthermore, the communication overheads of filter distribution are massively reduced since the filters are purposely distributed rather than random or epidemic distribution. The scheme in [15] uses fewer filters according to the increasing number of common attributes as shown in Fig. 5a, while it maintains the network overhead (Fig. 5b). In Fig. 5c, the number of blocked spam packets increases with an increasing number of common attributes.

To preserve a user's privacy, the distributed filters, including the key word of the creator's preferences, are encrypted in ciphertext where bilinear pairing techniques are utilized. At the beginning, the filter creator u_i chooses a random number $x_i \in \mathbb{Z}_q^*$ as the private key SK_i and computes her public key $PK_i = 1/x_iP$. The filter of u_i's key word W_k is $\mathcal{F}_{u_i,k} = < \mathcal{W}_{u_i,k}, \lambda_0 >$, where

$$W_{u_i,k} = \frac{H_1(W_k)}{x_i + H_1(W_k)} P, \lambda_0 = e(PK_i, P).$$

Then $\mathcal{F}_{u_i,k}$ is distributed to u_i's social friends. Her social friends could be honest but curious users. When a content source u_s sends a packet with key word W_x to u_i and finds u_j as a potential relay, u_j could help u_i detect whether or not this packet is desirable. Here, W_x is encrypted as $\Lambda_s = \lambda_1 + PK_i$, and

$$\lambda_1 = \frac{1}{H_1(W_x)} P.$$

Then u_j checks $e(\Lambda_s, \mathcal{W}_{u_i,k}) \stackrel{?}{=} \lambda_0$. If it holds, the keyword W_x passes the filter check, and the packet can be forwarded by u_j; otherwise, this packet will be blocked. Therefore, the private contents (i.e., the key word in the filter) are encrypted and protected from exposure to other users.

To resist the filter forgery attack, a Merkle hash tree is utilized to authenticate the filters from the creator u_i. Specifically, u_i sets her key word list $\mathcal{W}_{u_i} = W_{u_i,1}, \ldots, W_{u_i,K}$, where $W_{u_i,k}$ $(1 \leqslant k \leqslant K)$ is the key word selected by u_i, and located as a leaf node in filter tree $\mathcal{FR}_{u_i}$. During the authentication, the unique path information $\mathcal{PH}_k$ from the leaf node to the root node is used as the certificate for each independent key word (leaf node). Other users check whether or not the concatenated hash value of $\mathcal{PH}_k$ is equal to the root R_{u_i}. With this scheme, the filter forgery attack is defended in the spam content filtering.

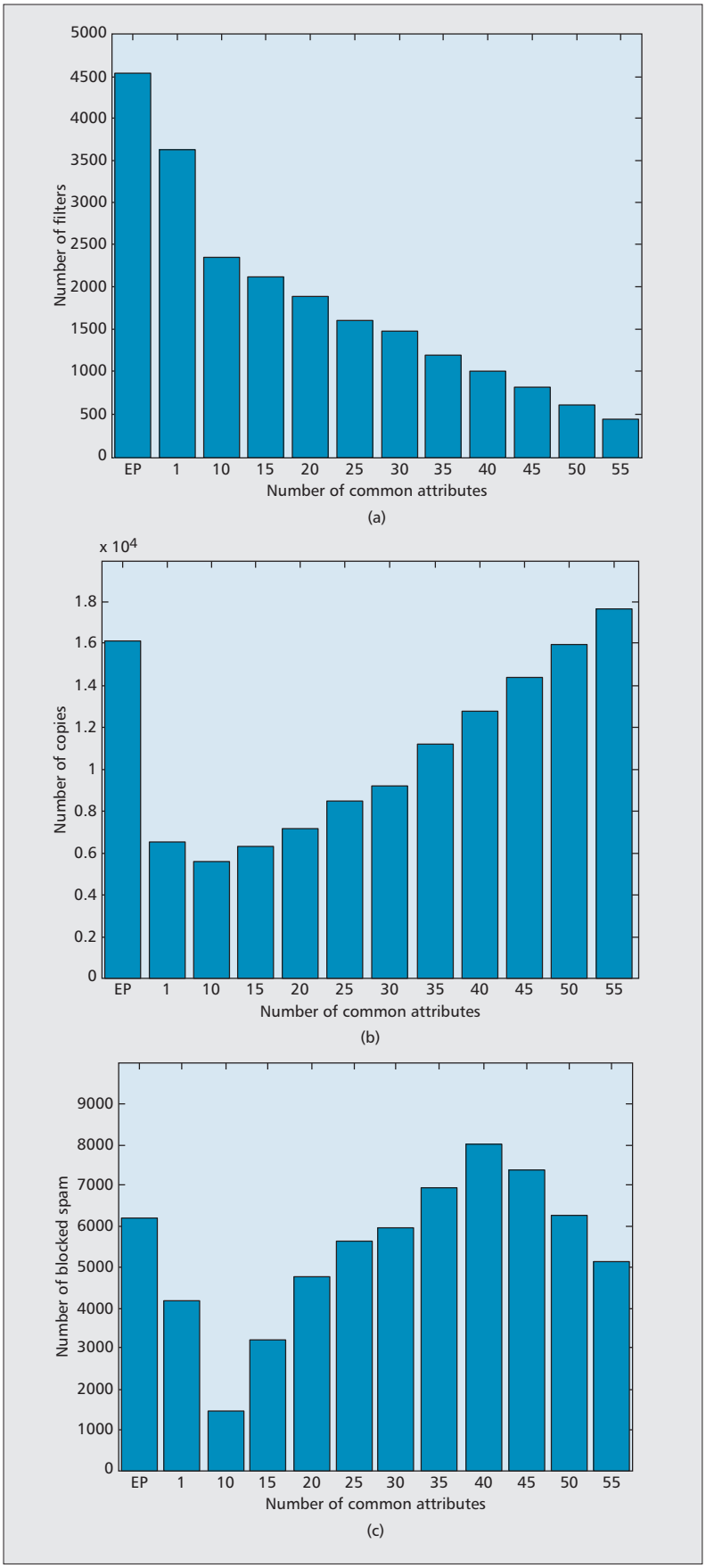

Figure 5. *Performance comparison. EP denotes the epidemic filter distribution (distribute to every encountered user). TH is the number of common attributes between the filter creator and the holders: a) number of filters vs.* TH*; b) number of copies vs. TH; c) number of blocked packets vs. TH.*

Research Challenges

In this section, we present some key issues and research directions related to security and privacy in an MMSN.

Privacy and Anonymity in Multimedia

The multimedia may contain some personalized contents in some cases. For example, a user's identity may be included in the generation process of a specific data format; a user's voice may be contained in an audio file; and a user's photo may appear in a shared picture or video. It is easy to share such personalized information in multimedia services, and a user's privacy would be violated. Therefore, privacy and anonymity in multimedia needs considerable research efforts. Some existing privacy preservation techniques, such as the pseudonym technique and secure multi-party computation, can protect the user's identity and unique information from disclosure in peer-to-peer information exchange. However, to preserve privacy in shared multimedia such as pictures, audio, and videos is still challenging. It is possible to enable content owners to manually remove or blur other users' unique information, including identities and portraits, before sharing the contents. An intelligent anonymization technique to handle images, audio, and video formats should be developed and adopted in MMSNs. Alternatively, the access policy should be defined and strictly followed. Only authorized users, such as trusted social friends, can obtain the shared contents, and should keep the contents confidential to strangers. Therefore, multidisciplinary research efforts should be put toward privacy and anonymization in multimedia.

Multimedia-Related Mobile Sybil Defense

In the multimedia content evaluation application, multimedia content reviews can provide a guideline for users to quickly make a judgement as to whether or not they are interested in multimedia content. However, malicious reviews might misguide users to make incorrect choices and degrade users' experiences. Particularly, multiple malicious users might collude to launch an enhanced Sybil attack. In addition, due to a mobile user's dynamically changing properties in an MMSN, mobile users' information and social structures cannot easily be obtained by a Sybil defender compared to that in online social networks (OSNs). Furthermore, without a centralized trusted authority, users may not be willing to provide their information and social relationships for Sybil defense. As a result, Sybil defense in MMSNs would be more challenging than that in OSNs, as depicted in Table 1. To this end, learning techniques and sociology can be further explored to assist in Sybil defense. Usually, Sybil attackers have some specific social behaviors (e.g., purposely producing malicious reviews on some specific multimedia content, or disseminating spam multimedia content), but inactively participating in normal user's activities. The disseminated and attacked multimedia content could also be investigated to link Sybil attackers. Moreover, mobile users could cooperate with trusted social friends to detect misbehaving Sybil attackers. The privacy leakage among trusted

social friends would be significantly reduced, while cooperation facilitates Sybil defense.

Conclusion

In this article, we have introduced the MMSN architecture and identified the security and privacy challenges. Furthermore, we have presented three MMSN applications, and addressed the security and privacy issues with supporting effective countermeasures, including privacy of content query, trust-based service evaluation, and privacy-preserving content filtering. Finally, we have presented future research directions with respect to privacy and anonymity in multimedia and multimedia-related mobile Sybil defense. We envision that this research should benefit both service providers and users in secure and privacy-preserving MMSNs.

Acknowledgment

This research has been supported by a research grant from the Natural Science and Engineering Research Council (NSERC), Canada.

References

[1] K. Lin *et al.*, "SocioNet: A Social-Based Multimedia Access System for Unstructured P2P Networks," *IEEE Trans. Parallel Distrib. Sys.*, vol. 21, no. 7, 2010, pp. 1027–41.

[2] G. Cardone *et al.*, "Socio-Technical Awareness to Support Recommendation and Efficient Delivery of IMS-Enabled Mobile Services," *IEEE Commun. Mag.*, vol. 50, no. 6, 2012, pp. 82–90.

[3] I. Roussaki *et al.*, "Context-Awareness in Wireless and Mobile Computing Revisited to Embrace Social Networking," *IEEE Commun. Mag.*, vol. 50, no. 6, 2012, pp. 74–81.

[4] X. Liang *et al.*, "Security and Privacy in Mobile Social Network and Applications: Challenges and Solutions," *IEEE Wireless Commun.*, to appear.

[5] J. Troncoso-Pastoriza and F. Perez-Gonzalez, "Secure Signal Processing in the Cloud: Enabling Technologies for Privacy-Preserving Multimedia Cloud Processing," *IEEE Sig. Process. Mag.*, vol. 30, no. 2, 2013, pp. 29–41.

[6] Y. Wu, Z. Wei, and R. Deng, "Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks," *IEEE Trans. Multimedia*, vol. 15, no. 4, 2013, pp. 778–88.

[7] M. Li *et al.*, "FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks," *Proc. IEEE INFOCOM*, 2011, pp. 2435–43.

[8] H. Shen and G. Liu, "An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing," *IEEE Trans. Parallel Distrib. Sys.*, to appear.

[9] L. Cutillo, R. Molva, and T. Strufe, "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust," *IEEE Commun. Mag.*, vol. 47, no. 12, 2009, pp. 94–101.

[10] X. Liang, X. Lin, and X. Shen, "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks," *IEEE Trans. Parallel Distrib. Sys.*, vol. 25, no. 2, 2014, pp. 310–20.

[11] H. Wang *et al.*, "Accelerating Peer-to-Peer File Sharing with Social Relations," *IEEE JSAC*, vol. 31, no. 9, 2013, pp. 66–74.

[12] H. Zhao, W. Lin, and K. Liu, "Cooperation and Coalition in Multimedia Fingerprinting Colluder Social Networks," *IEEE Trans. Multimedia*, vol. 14, no. 3, 2012, pp. 717–33.

[13] D. Boneh and B. Waters, "Conjunctive, Subset, and Range Queries on Encrypted Data," *IACR Crypto. ePrint Archive*, vol. 2006, 2006, p. 287.

	MMSN	OSN
Dynamic	Yes	No
Centralized Sybil defense	No	Yes
Collusion	Yes	Yes
Long-term behavior statistic	No	Yes

Table 1. *Sybil defense in MMSN and OSN.*

[14] M. Wen *et al.*, "PaRQ: A Privacy-Preserving Range Query Scheme over Encrypted Metering Data for Smart Grid," *IEEE Trans. Emerg. Topics Comp.*, vol. 1, no. 1, 2013, pp. 178–91.

[15] K. Zhang *et al.*, "SAFE: A Social Based Updatable Filtering Protocol with Privacy-Preserving in Mobile Social Networks," *Proc. IEEE ICC*, 2013, pp. 6045–49.

Biographies

Kuan Zhang [S'13] (k52zhang@bbcr.uwaterloo.ca) received his B.Sc. degree in electrical and computer engineering and M.Sc. degree in computer science from Northeastern University, China, in 2009 and 2011, respectively. He is currently working toward a Ph.D. degree with the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include security and privacy for mobile social networks.

Xiaohui Liang [S'10] (x27liang@bbcr.uwaterloo.ca) is currently working as a postdoctoral fellow with the BBCR Group, University of Waterloo. He received his Ph.D. degree from the Department of Electrical and Computer Engineering of the University of Waterloo, and his Master and Bachelor degrees from the Computer Science Department of Shanghai Jiao Tong University, China. His research interests include security and privacy for e-healthcare systems and mobile social networks.

Rongxing Lu [S'09, M'11] (rxlu@ntu.edu.sg) received his Ph.D. degree in computer science from Shanghai Jiao Tong University in 2006, and his Ph.D. degree (awarded the Canada Governor General Gold Medal) in electrical and computer engineering from the University of Waterloo in 2012. From May 2012 to April 2013, he worked as a postdoctoral fellow at the University of Waterloo. Since May 2013, he has been an assistant professor at the School of Electrical and Electronics Engineering, Nanyang Technological University. His research interests include computer network security, mobile and wireless communication security, and applied cryptography.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] (xshen@bbcr.uwaterloo.ca) is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. He was the Associate Chair for Graduate Studies from 2004 to 2008. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He served as the Technical Program Committee Chair/Co-Chair for IEEE INFOCOM '14, IEEE VTC '10 Fall, Symposia Chair for IEEE ICC '10, Tutorial Chair for IEEE VTC '11 Spring and IEEE ICC'08, and Technical Program Committee Chair for IEEE GLOBECOM '07. He also serves/served as Editor-in-Chief for *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology and Communications Societies.

We have presented future research directions with respect to privacy and anonymity in multimedia and multimedia-related mobile Sybil defense. We envision that this research should benefit both service providers and users in secure and privacy-preserving MMSN.