SECURITY AND PRIVACY IN MOBILE SOCIAL NETWORKS: CHALLENGES AND SOLUTIONS

XIAOHUI LIANG, KUAN ZHANG, AND XUEMIN SHEN, UNIVERSITY OF WATERLOO
XIAODONG LIN, UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY

ABSTRACT

Mobile social networking is a pervasive communication platform where users with smartphones can search over the Internet and query neighboring peers to obtain the desired information. In this article, we examine the architecture, communication patterns, and especially the security and privacy of MSN. We first study three categories of mobile applications with a focus on two autonomous mobile applications, business card and service review. We then explore the possible methods to deal with the associated security and privacy challenges. By discussing the shortages of the methods, we finally provide several promising research directions.

INTRODUCTION

As reported by ComScore [1], social networking sites such as Facebook and Twitter have reached 84 percent of the world's online population, representing 1.3 billion users around the world. In the meantime, fueled by the dramatic advancements of smartphones and the ubiquitous connections of Internet networks, social networking further becomes available for mobile users and keeps them posted on up-to-date worldwide news and messages from their friends and families anytime anywhere. The convergence of social networking, advanced smartphones, and stable network infrastructures brings us a pervasive and omnipotent communication platform, mobile social networking (MSN), helping us stay connected better than ever.

The boom of mobile applications is one of the important factors in MSN development. It is reported from WiKi that Apple Inc. has greatly increased the number of mobile applications from 800 in July 2008 to over 825,000 in April 2013. Generally, these mobile applications can be divided into three categories. The first category is mobile versions of online social applications (OSAs), which enable users to check social updates, share photos, and watch online videos in a mobile environment. The communications remain between smartphone users (SUs) and Internet service providers (ISPs). Web-based/password-based authentication can be continuously applied to prevent SUs' content from being accessed by unauthorized entities. Security and privacy are not difficult to solve because the ISPs are fully trusted by the SUs. In addition to voice service available for any cellular telephone, smartphones distinguish themselves by powerful computing resources and, most significantly, their capability to understand their surrounding environments through many sensors that are built into them. As a result, the second category, location-based applications, becomes one of the most popular. It utilizes the information downloaded from the Internet to assist location-based activities. Such applications are widely supported by either social network giants like Facebook or specialized service providers like Foursquare and Loopt. The main idea is as follows: The GPS chips detect the location coordinates of the SUs, who then report the coordinates to the ISPs for downloading the information related to local services. However, it raises a serious privacy issue; the continuously disclosed location coordinates may reveal where, when, or even what SUs have done. To prevent abuse of their location coordinates, SUs have to often manually switch localization on and off to control access to their location information. The third category is autonomous mobile applications, where SUs are able to connect to neighboring SUs and local service providers (LSPs) through short-range wireless communications such as near field communication (NFC), Bluetooth, and WiFi Direct. For example, a nearby information search application [2] helps an SU consult her nearby friends, who in turn will ask their friends, and so on, until the information is found. In this application, the SUs are not required to have an Internet connection. Besides, navigating for information via neighboring SUs could be better than Internet search because the information from a neighborhood is often more personalized, localized, and up-to-date. Autonomous mobile applications can also be applied to facilitate car pool [3] and healthcare purposes. However, the security and privacy of such applications are very challenging. In fact, SUs are unlikely to share their privacy-sensitive destinations or healthcare symptoms with strangers. Without a trust mediator, the privacy is easily violated, and thus the SUs are probably uncooperative.

1536-1284/14/$25.00

The static LSP is equipped with enhanced communication and storage devices that are placed on, in or around their buildings. The LSPs could use these communication devices to interact with the nearby SUs. For example, a restaurant is always interested in disseminating its promotion to the potential customers.

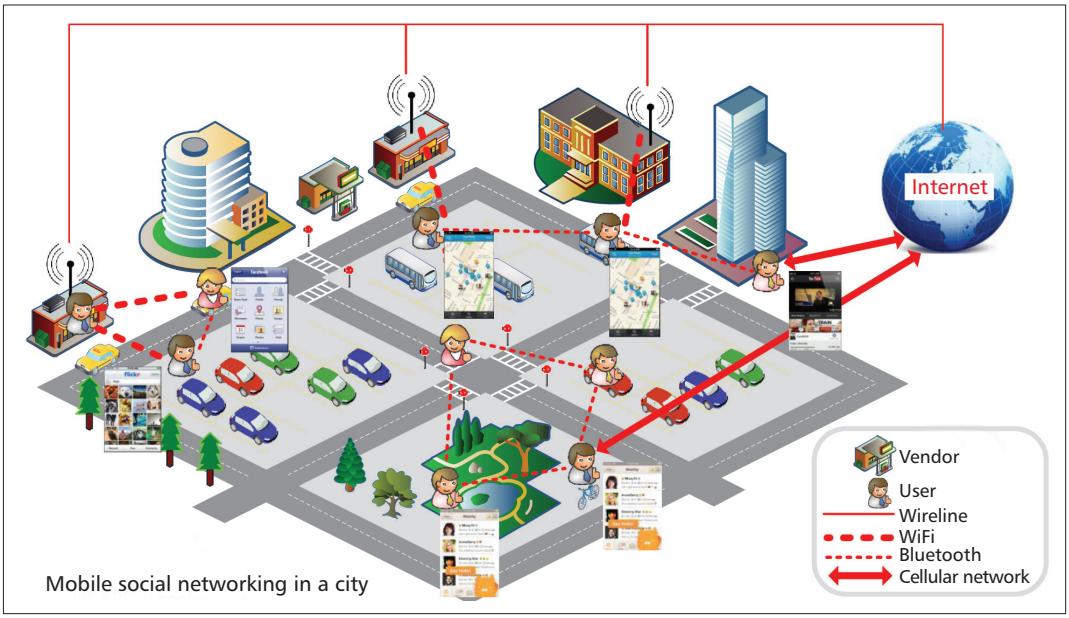

Figure 1. *MSN architecture. The SUs have various communication technologies to reach the ISPs, the LSPs, and other SUs. Mobile applications enable the SUs to watch online videos (Youtube), update personal information (Facebook), share photos (Flickr), search for information (Foursquare), and talk to neighbors (SayHello) anytime anywhere.*

As indicated above, despite the tremendous benefits brought by MSN and its applications, MSN still faces many security and privacy challenges, including private information leakage, cheating detection, Sybil attacks, and so on. Recently, extensive research efforts [4–6] have been made to deal with these research challenges by exploring the unique MSN characteristics. However, the overall architecture and social impact from the security and privacy perspective have not been systematically studied. Clearly, to study the security and privacy requirements and their relations to the unique MSN characteristics is very critical before any specific scheme design. In this article, we first define an overall MSN architecture with the communication entities and the communication patterns. We then explore the security and privacy requirements with the associated social factors. In addition, we describe three categories of applications and their associated research challenges and solutions. Lastly, we present some promising future research directions.

MSN Architecture

In this section, we present MSN architecture by introducing the communication entities, the communication patterns, and the security and privacy requirements [7].

MSN Communication Entities

An MSN, as shown in Fig. 1, is a virtual environment composed of the SUs moving in a local geographical area, the LSPs, and the ISPs. It is formed upon the agreement of the participating SUs and LSPs.

Smartphone Users — The SUs are able to not only access the Internet via cellular/WiFi networks, but also communicate with neighboring SUs via Bluetooth/NFC technologies. The SUs choose the communication technologies for different applications. For example, the SUs may choose the Internet to obtain service information, and use Bluetooth to communicate with nearby SUs to obtain service reviews. The SUs also consider their mobility and social behavior patterns when choosing the communication technologies.

Local Service Providers — The LSPs, either mobile or static, provide services to the SUs in the vicinity. When an LSP is mobile, it can be equipped with a smartphone that disseminates service information to the encountered SUs. When an LSP is static, it could be in a local store or restaurant that is visited by nearby SUs. A static LSP is equipped with enhanced communication and storage devices that are placed on, in, or around their buildings. The LSPs could use these communication devices to interact with nearby SUs. For example, a restaurant is always interested in disseminating its promotion to potential customers.

Internet Service Providers — Mobile access to Internet service is available due to the pervasive deployment of cellular network infrastructures. Besides, SUs can also access the Internet via WiFi hotspots, which are widely distributed in restaurants, shopping malls, and even residential communities. As a result, the ISPs can be reached almost anytime anywhere. They can also provide service information to SUs in MSN whenever and wherever the SUs need it.

MSN Communication Patterns and Techniques

The communication patterns in MSN are generally divided into SU-to-ISP, SU-to-LSP, and SU-to-SU categories.

SU-to-ISP — Two common communication technologies that are enabled on smartphones help SU-to-ISP communications. One is cellular networks. The SUs purchase a data plan from wireless carriers, such as Rogers and Verizon. Their smartphones can connect to the Internet through the cellular network infrastructures maintained by these companies. For example, SUs spend $5/$17/$37 to purchase a monthly plan which provides 10 Mbytes/250 Mbytes/5 Gbytes Internet data to their smartphones. The other one is WiFi technology. Compared to the previous, WiFi technology can offer pervasive Internet access at cheaper costs and larger bandwidth. Many LSPs integrate free WiFi access into their commercial business solutions. For example, the Canada-wide coffee shop Tim Hortons chain have worked with Bell Canada to roll out the national free WiFi service to more than 2000 Tim Hortons locations since September 2012. In addition, more and more commercial solutions are developed by companies like FatPort and Fon, encouraging distributed WiFi hotspots to cooperatively share Internet access with nearby SUs.

SU-to-LSP — SU-and-LSP communications help SUs better obtain the service information of nearby LSPs. The communications can be done by short-range wireless technologies, such as WiFi and Bluetooth. Due to the ease of setup and low costs, many LSPs have been equipped with wireless routers to offer Internet access to their customers. In other words, these LSPs are connected to their customers through WiFi. In addition, when the LSPs are mobile, they can also be equipped with short-range communication devices and send the service information to the encountered SUs via Bluetooth.

SU-to-SU — When SUs launch autonomous mobile applications, SU-to-SU communication is useful for the SUs to share information efficiently. Short-range communication technologies like NFC, Bluetooth, and WiFi Direct are integrated into smartphones to implement SU-to-SU communication. NFC operates at slower speeds than Bluetooth, but consumes far less power without pairing. NFC sets up more quickly than standard Bluetooth, but has a lower transfer rate than Bluetooth Low Energy. With a maximum working distance of less than 20 cm, NFC has a shorter range, which reduces the likelihood of unwanted interception. It makes NFC particularly suitable for crowded areas. In comparison, Bluetooth and WiFi Direct support longer wireless communication ranges more suitable for SUs to share information over distance. In addition, WiFi Direct promises data transfer speeds of up to 250 Mb/s, much faster than Bluetooth and NFC, but consuming more energy.

MSN Security and Privacy

MSN security and privacy are urgent research issues once various MSN applications are widely launched in an insecure MSN environment. The emerging security and privacy issues of MSN are tightly related to the specific application design and a user's unique requirements. Generally, when we design MSN applications, we should consider trust relations, private information leakage, and malicious behavior. In the following, we first introduce these security and privacy issues, and then discuss them in different applications.

Trust Relations — Trust relation is a fundamental part of mobile applications. Mobile applications can only be adopted by SUs if the SUs have trust in the ISPs, LSPs, and other SUs. While SUs enjoy the conveniences brought by mobile applications maintained by the ISPs, they realize that more and more personal information is revealed to the ISPs and start questioning how the ISPs keep the collected personal information, and whether the ISPs disclose the information for other purposes without proper consent. Some research works [8, 9] suggest that SUs only disclose fuzzy identity and location information to the ISPs.

A social community is a platform to build social relations among people who share interests, activities, backgrounds, or real-life connections. In MSN, social community implies trust relationships, and helps SUs and LSPs build trust relationships in a distributed way. When two SUs know that they belong to the same social community (university or company) or have some common interests (sports or tastes), each has a feeling that the other is more reliable, and the shared opinions are more trustful. Some research works [4–6] develop privacy-preserving profile matching protocols to help two SUs obtain their common interests. Besides, social ties representing the relationships between two SUs are the foundation for effective collaboration. In MSN, the strength of social ties can be used to facilitate effective data forwarding [10, 11] and service recommendation [12].

Private Information Leakage — Private information, such as identities, pseudonyms, locations, and profiles, may be revealed in most mobile applications to some extent. In fact, social networking plus mobile applications can easily be used to trace an SU's behavior if the SU does not intentionally protect himself. Popular social applications like Facebook and Twitter have deliberate privacy settings, while others may not provide adequate protection. However, in practice, most SUs choose to ignore the privacy settings and put themselves in potential danger. Recent research works [10] suggest the use of historical social contacts to facilitate the packet forwarding in the future, while not considering that the social contacts, including identities, are privacy-sensitive to SUs and could be never shared by SUs. As an effective solution, the profile matching protocols [4–6] would help users only reveal the privacy-preserving matching results.

Malicious Behavior — Most autonomous mobile applications are ineffective in the presence of SUs' malicious behavior. For example, in cooperative packet forwarding, if every SU always expects others' help but refuses to help others, cooperative packet forwarding may never succeed; in the trustworthy service evaluation (TSE) system, if the LSPs and SUs can arbitrarily add positive reviews and delete negative reviews, the

The emerging security and privacy issues of MSN are tightly related to the specific application design and the user's unique requirements. Generally, when we design MSN applications, we should consider the trust relations, the private information leakage, and the malicious behavior.

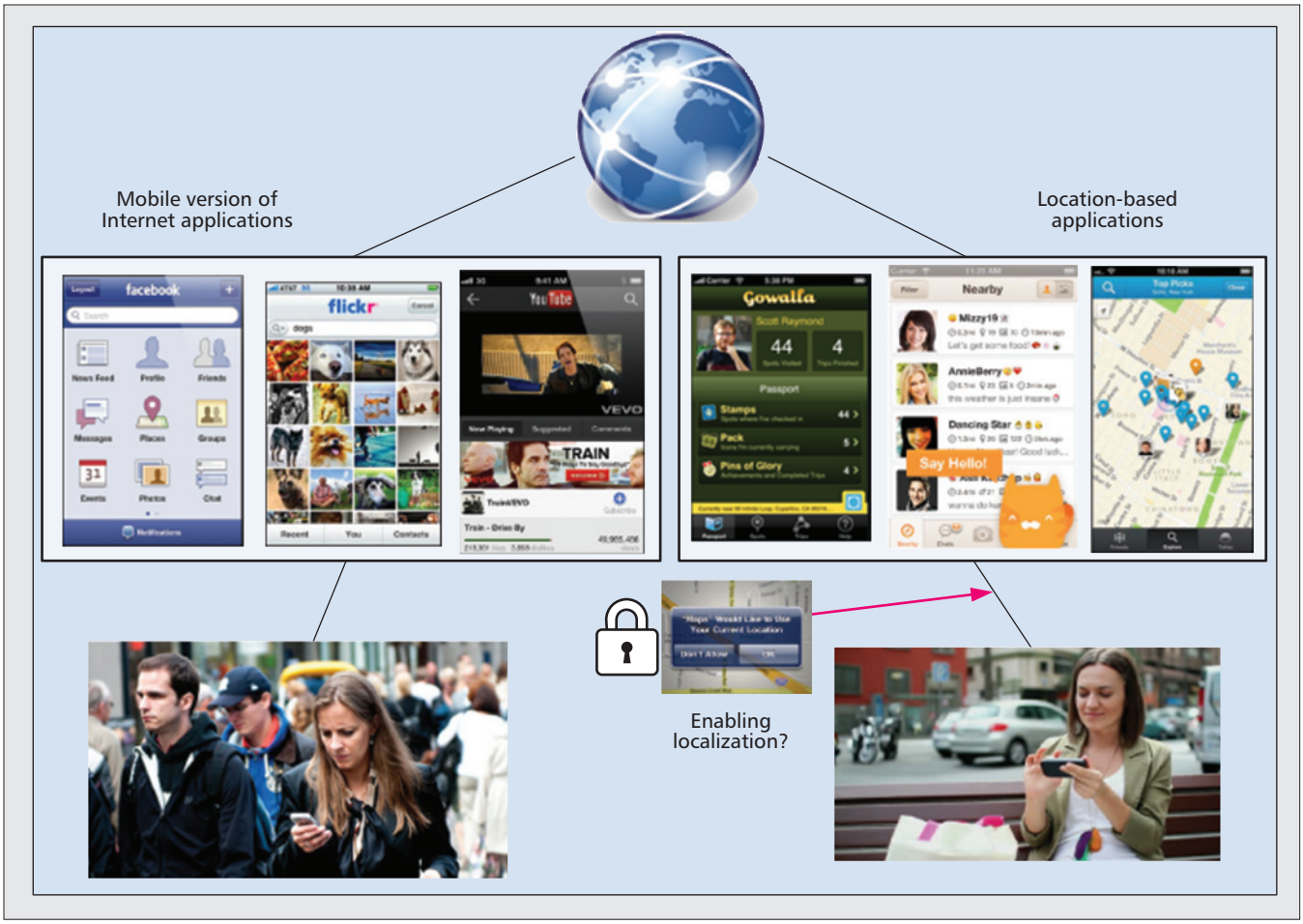

Figure 2. *Mobile version of online social applications and location-based applications.*

SUs cannot receive authentic and useful reviews, and stop running the applications. Some research works [10, 11] consider social selfishness and social morality into the calculation of utility, and explore novel packet forwarding protocols. Some research work [12] studies review attacks and Sybil attacks, and propose corresponding defensive mechanisms in the distributed TSE system.

MSN Applications

In this section, we briefly introduce the mobile version of online social applications and location-based applications, and then focus on two autonomous mobile applications.

Mobile Versions of Online Social Applications

Successful OSAs such as Facebook and Youtube have been extended to mobile versions. Nowadays, hardware specifications of smartphones are comparable to those of personal computers, along with friendly interface improvements and usability enhancements. Moreover, the deployment of third generation (3G) and Long Term Evolution (LTE) networks has considerably improved the available mobile bandwidth, enabling provisioning of content and services powered by ISPs. When SUs launch the applications, they are able to quickly download/upload data from/to the ISPs. As such, a security issue has been raised; that is, SUs have the capability to send information out to the world in an easy and fast way, such as updating status or changing a head photo. Anyone with Internet access is able to keep tracking the SUs' behavior, which is extremely dangerous. As such, when sharing information, SUs need to be mindful about whether personal information disclosure is necessary or not.

Location-Based Applications

Foursquare is a typical location-based application that allows registered users to post their locations at a venue ("check in") and connect with friends. One can check in to a certain floor/area of a building, or indicate a specific activity while at a venue. Users can choose to have their check-ins posted on their accounts on Twitter or Facebook. The location-based application collects and utilizes locations, which are most privacy-sensitive to SUs. Inappropriate disclosure of locations to potential attackers may put the SUs' lives in danger or cause property loss. In practice, SUs often trust LSPs. It is common that some locations have to be disclosed for exchanging with valuable local service information. However, SUs should still have control over how precise a level of location information is disclosed and how much personal information is linked to those locations. In the current applica-

Figure 3. *Business card application.*

tions, the location coordinates of SUs are directly reported to service providers. Instead, SUs may only reveal a geographic area that circle around the precise coordinate or mix their identities with nearby SUs [8, 9]. Besides, when registering with the applications, SUs can provide limited personal information and carefully define which part of the information can be shared with whom.

Autonomous Mobile Applications

Autonomous mobile applications can be developed for many interesting and specific scenarios. We introduce two autonomous mobile applications: business card and service review, both of which are launched in an insecure and distributed environment.

business card application: Exchanging business cards in a public place, such as conference sites and restaurants, is a very common social activity when users want to introduce themselves to nearby others. In practice, users do not arbitrarily choose neighbors to whom to give out their business cards. They usually chat with others for a while and get to know others' backgrounds. If they need to know further details or keep in touch with others in the future, they exchange business cards for more effective communications.

In MSN, with smartphones, SUs have another option: to exchange electronic business cards (e-cards) that are preset in their smartphones, as shown in Fig. 3. The e-card application is easy to use and cost saving. However, it has two design challenges:

- Verification that an e-card is not forged
- Ensuring that only a designated SU, not others, can receive it

The first challenge can be solved via the help of an authoritative entity who generates a digital signature on each e-card. SUs must provide the signature with the e-cards at the same time. For the second challenge, NFC technology could be a solution where two SUs need to be physically contacted and put their smartphones at a distance no more than 20 cm. Bluetooth is an alternative that enables two SUs with further distance to share e-cards. In this case, before exchanging e-cards, two SUs need to check if the other is the one with whom they wish to communicate. Even with simple authentication provided by NFC/Bluetooth, SUs could still wrongly connect their phones with other malicious attackers.

Inspired by the traditional way of exchanging business cards, we introduce a novel gesture-based authentication scheme for the e-card application. The scheme requires each SU to perform a gesture at the beginning. The gestures are as simple as shaking the smartphone in an up, down, left, or right direction, or a composition of these simple gestures. Two SUs both need to repeat each other's gestures and send the gesture information back to the original SU. After confirming the right gesture, the original SU sends the e-card. The gesture-based authentication scheme takes gestures as a temporary password that can be obtained by only close-enough SUs with visibility. Without seeing and repeating the gestures, other malicious attackers are unable to eavesdrop the e-cards. In this way, the SUs can have secure and efficient e-card sharing. Table 1 shows the comparison between password-based and gesture-based authentications.

Service review application: Over the Internet, many social and online shopping sites allow customers to write service reviews of a specific service or product. From the review systems, service providers could know the user experiences and be able to improve service quality right away. Besides, the reviews from others could be very helpful for users to decide which service/product they should choose. The use of such systems is a common social activity where users freely share service reviews as recommendations for friends. Nowadays, most companies have already inte-

Over the Internet, many social and online shopping sites allow customers to write service reviews of a specific service or product. From the review systems, service providers could know the user experiences and be able to improve service quality right away.

grated the review system as an important advertising tool to boost their global market.

In MSN, LSPs such as restaurants and grocery stores offer local services to nearby SUs. There is a need for LSPs and SUs to exchange information. The LSPs want to disseminate service information to the SUs, such as their locations and flyers, while the SUs want to know the service information. In addition, the service reviews of friends play an important role in the SUs' service selection. In MSN, the service review application aims to help two SUs directly share reviews or indirectly via the LSPs, as shown in Fig. 4.

Direct service review sharing. When two SUs both have visited or are about to visit an unfamiliar LSP, they need to communicate with each other, expecting to know more about the LSP. For example, one SU may want to know from the other if the service is good in an automobile dealership before having a car fixed there or whether the food is delicious in a restaurant before randomly picking a dish with a "delicious" name. However, different experiences and different backgrounds of SUs may result in distinctive service reviews. A profile matching technique can be used to enable two SUs to check if they have some interests in common before sharing reviews. According to interest categorization, service reviews are more valuable and trustworthy to SUs. Although profile matching is helpful, it should not over-disclose SUs' private profile information [4–6].

Indirect service review sharing. Due to mobility, direct sharing may not always be enabled among the SUs. We introduce a TSE system [12] that helps the SUs indirectly share their service reviews via the LSP. It works in the following way. The SUs cooperatively upload their service reviews to the TSE system, which is maintained by the LSP. Then the LSP disseminates the service reviews to other SUs. However, since the LSP may launch some malicious attacks to modify the review collections, the SUs need to authenticate the received reviews. One solution is to utilize the aggregate signature to build the review collection [12]. Consider multiple SUs $\{SU_1, SU_2, \cdots, SU_n\}$ generating service reviews $R_1, R_2, \cdots, R_n$, respectively. For each review R_i, to protect the review's integrity, SU_i generates a signature on $S_i = Sign(psk_i, R_i)$, where psk_i is a pseudonym secret key corresponding to the pseudonym pid_i. psk_i, and pid_i are generated by a centralized identity-based cryptosystem. Note that if SU_i submits (R_i, S_i) to the TSE system, the LSP can easily delete any review without being detected. However, when aggregate signature is applied, $\{S_1, S_2, \cdots, S_n\}$ are aggregated into one signature $\bar{S}$. By the cooperation from the SUs, the review collection is converted from $(R_1, \cdots, R_n, S_1, \cdots, S_n)$ to $(R_1, \cdots, R_n, \bar{S})$. In this way, the LSP either deletes or keeps the whole review collection. It can be seen that the reviews are integrated and the modification capability of the LSP is reduced. In [12], review rejection attacks of the TSE system has been studied in a simulated MSN. Each review has a value in [0, 1]. A review is negative if its value is lower than 0.5. The vendor performs review rejection attacks by rejecting all negative reviews. When multiple reviews are aggregated and submitted together, the vendor accepts them if the average value is no less than 0.5, or rejects them otherwise. Multiple tokens are circulated among users to help them aggregate reviews. Figure 5a shows the comparison of submission rates of the basic TSE (bTSE) system and the non-cooperative system under no review rejection attacks and different service ranges (SRs), while Fig. 5b shows the results under attack. It can be seen that when the review rejection attacks do not exist, the bTSE and non-cooperative systems achieve similar submission rates. When review rejection attacks exist, the bTSE system achieves a significantly higher submission rate than the non-cooperative system, up to 100 percent. The simulation results clearly indicate that the bTSE system is able to effectively resist review rejection attack.

	Password	Gesture
Complexity	High	Low
Update	Per user	Per session
Channel	Wireless	Optical
Need to be memorized	Yes	No
Usability	Hard	Easy

Table 1. *Comparison between two authentication methods.*

The service review application can be further extended in a *multihop version*, as shown in Fig. 4b. When an SU receives a service review, it can further share the review with other encountered SUs. Multihop service review dissemination helps SUs obtain more information about the services. However, it may have a trustworthy issue; that is, the service review may be modified and its credibility reduced after multihop transmission. The trust and recommendation mechanism [13] of the information propagation can be considered in the design of dissemination methods. In addition, the incentive and effectiveness of multihop dissemination has also attracted many research efforts [6, 10, 14]. Besides, *disseminators* are communication devices that are set up by the LSPs or a government facility. They could be integrated into the service review application. In real life, we often see billboards placed at a crossroad near a mall. Billboards help nearby users know what services are provided in the mall. In MSN, disseminators can be put on billboards to help exchange up-to-date service information and service reviews from LSPs and SUs. The sooner SUs receive the information, the better service the SUs can choose, and the more potential customers the LSPs have.

Research Challenges

As MSN is essentially built in the broad field of open wireless medium, it inherits a variety of fundamental security problems such as data eavesdropping attacks, secure routing, and

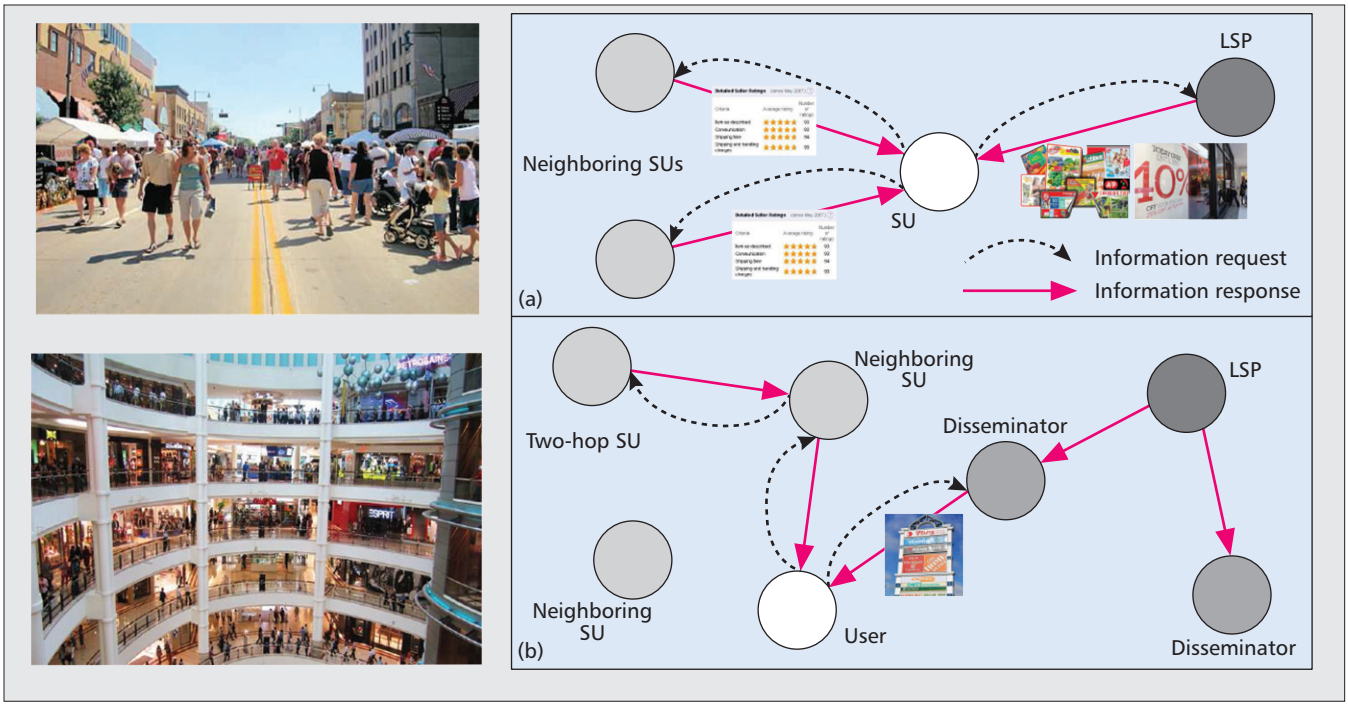

Figure 4. *Service review application.*

denial-of-service attacks. Given the limited space, we address the following challenges.

Gesture-Assisted Secure Information Sharing

Previously, we introduced the promising business card application, which is a common social activity in real life. With smartphones, our capabilities in sensing and communication are significantly improved, and our social activities are carried out in a more efficient way. However, due to the broadcast nature of the wireless medium, it is very difficult to negotiate a shared secret and implement secure information sharing if two SUs have no pre-established knowledge of each other. Gesture-based information sharing is a unique research direction in MSN. The gesture information is only visible to neighbors who are close enough. SUs can make simple gestures clear enough that a target SU can repeat it. In order to achieve secure information sharing, the gesture can be changed for each session. In the meantime, accelerometer sensors and gyroscope sensors can also be used to detect gestures and check if two gestures are the same. One interesting research direction is discovering how to limit the physical and visual spaces such that the gestures are only visible to the target SU. Besides, it is also interesting to explore more applications using gesture-assisted secure information sharing.

Social-Context-Based Private Information Management

The information to be shared by the SUs in MSN is closely related to the social context, including the profiles of neighboring SUs and the service of neighboring LSPs. For example, in a shopping mall, people surrounded by clothing stores expect to share and receive discount information on clothes; in a conference, participants are willing to discuss research topics and projects with other research scholars. Based on the social context, the disclosed personal information can be used to identify an SU's behavior at different levels. In the previous example, if a research scholar discusses research topics in a shopping mall, his behavior is easily distinguished from nearby customers. Thus, to achieve privacy preservation, the social context should be considered in MSN communication protocol design. Most existing privacy-preserving profile matching protocols [4, 5] aim at minimizing profile information disclosure but neglect the relations between the disclosed information and the social context. From [6], it is shown that the anonymity variation of an SU depends on the profile information of its nearby SUs. Thus, the effectiveness of profile matching protocols in terms of privacy preservation needs to be further validated in different social contexts. Exploring practical social contexts and proposing effective protocols for specific social contexts is an important research direction.

Effective Resistance to Mobile Sybil Attacks

Distributed systems are vulnerable to Sybil attacks where an attacker manipulates bogus identities or abuse pseudonyms to compromise the effectiveness of the systems. Especially for MSN, the SUs often adopt multiple pseudonyms for protecting their location privacy [6, 11]. Thus, it is very challenging to restrict Sybil attackers who legally have multiple pseudonyms but maliciously use them. In MSN, Sybil attacks can be further extended to the mobile version, called mobile Sybil attacks (MSAs), which can be launched by mobile SUs anytime anywhere. The MSAs are hardly to be detected because their behaviors are difficult to monitor. The previously introduced TSE system is

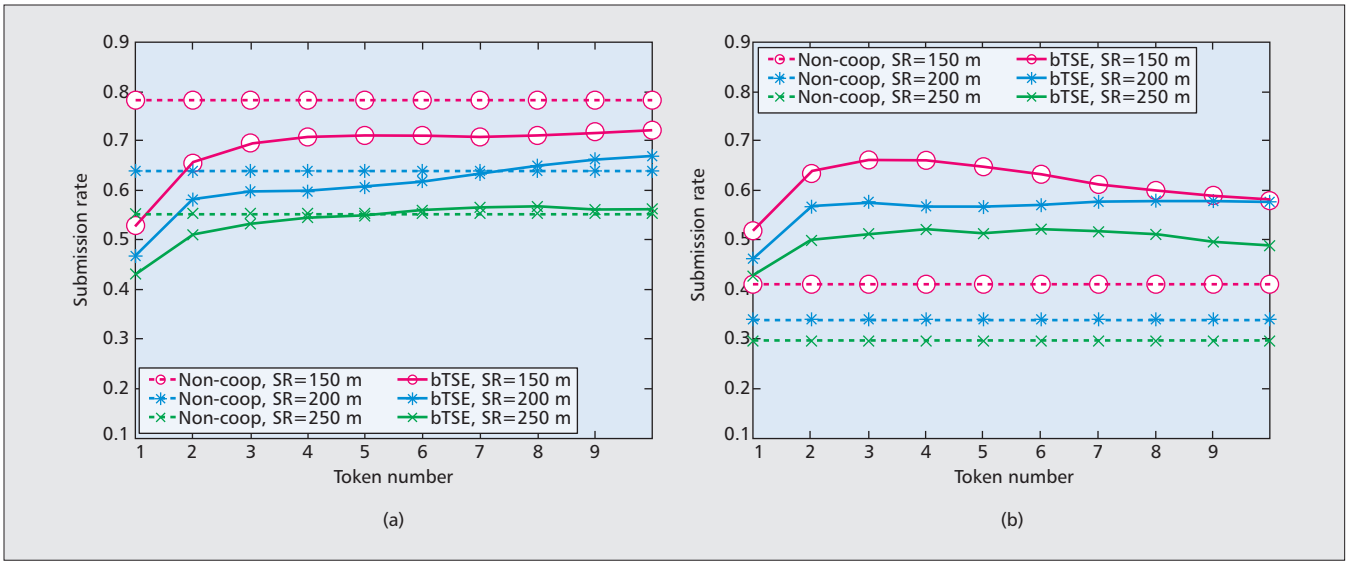

Figure 5. *Submission rate of TSE system in MSN [12]: a) no rejection attacks; b) under rejection attacks.*

subject to the MSAs [12]. One solution is pervasive and cooperative monitoring, that is, requiring normal SUs to monitor other SUs' behaviors and submit the monitoring results to a centralized authority. Then the centralized authority can correlate the results and detect MSAs by viewing the statistic information. This method is similar to traditional Sybil attack detection [15] in online social networks. However, in MSN, this method requires extensive communication overhead and incurs unexpected detection delay. Another solution [12] is to embed a secret in the multiple pseudonyms of one SU. When the attacker uses the pseudonyms beyond the predefined boundary, its real identity is calculated from these pseudonyms. In both solutions, how to define the boundary between MSAs and good behavior is challenging. Location information may be integrated into the boundary design of MSA detection.

Conclusion

In this article, we have studied the security and privacy issues in mobile social networking and applications. We have defined MSN communication patterns, and introduced the security and privacy challenges. We have also offered several promising approaches to deal with the security and privacy challenges in various mobile applications, especially for the business card and service review applications. Lastly, we have presented three promising research directions: gesture-assisted secure information sharing, social-context-based private information management, and effective resistance to mobile Sybil attacks.

References

[1] ComScore, http://www.comscoredatamine.com/.
[2] M. Motani, V. Srinivasan, and P. Nuggehalli, "Peoplenet: Engineering a Wireless Virtual Social Network," *Proc. MobiCom*, 2005, pp. 243–57.
[3] M. Brereton *e al.*, "Designing Participation in Agile Ridesharing with Mobile Social Software," Proc. Annual Conference of the Australian Computer-Human Interaction Special Interest Group, 2009, pp. 257–60.
[4] M. Li *et al.*, "Findu: Privacy-Preserving Personal Profile Matching in Mobile Social Networks," *Proc. IEEE INFOCOM*, 2011, pp. 2435–43.
[5] R. Zhang *et al.*, "Fine-Grained Private Matching for Proximity-Based Mobile Social Networking," *Proc. IEEE INFOCOM*, 2012, pp. 1969–77.
[6] X. Liang *et al.*, "Fully Anonymous Profile Matching in Mobile Social Networks," *IEEE JSAC*, vol. 31, no. 9, 2013, pp. 641–55.
[7] N. Kayastha *et al.*, "Applications, Architectures, and Protocol Design Issues for Mobile Social Networks: A Survey," *Proc. IEEE*, vol. 99, no. 12, 2011, pp. 2130–58.
[8] X. Zhao, L. Li, and G. Xue, "Checking In without Worries: Location Privacy in Location Based Social Networks," *Proc. IEEE INFOCOM*, 2013, pp. 3003–11.
[9] K. Puttaswamy *et al.*, "Preserving Location Privacy in Geo-Social Applications," *IEEE Trans. Mobile Computing*, 2013.
[10] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *Proc. IEEE INFOCOM*, 2010, pp. 857–65.
[11] X. Liang *et al.*, "Morality-Driven Data Forwarding with Privacy Preservation in Mobile Social Networks," *IEEE Trans. Vehic. Tech.*, vol. 7, no. 61, 2012, pp. 3209–22.
[12] X. Liang, X. Lin, and X. Shen, "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks," IEEE Trans. Parallel and Distributed Systems, 2013.
[13] A. Jøsang, R. Hayward, and S. Pope, "Trust Network Analysis with Subjective Logic," *Proc. Australasian Computer Science Conference*, 2006, pp. 85–94.
[14] G. Costantino, F. Martinelli, and P. Santi, "Investigating the Privacy vs. Forwarding Accuracy Tradeoff in Opportunistic Interest-casting," *IEEE Trans. Mobile Computing*, 2013.
[15] L. Shi *et al.*, "Sybilshield: An Agent-Aided Social Network-Based Sybil Defense among Multiple Communities," *Proc. IEEE INFOCOM*, 2013, pp. 1034–42.

Biographies

Xiaohui Liang [S'10, M'13] (x27liang@bbcr.uwaterloo.ca) is a postdoctoral fellow in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He obtained his Ph.D. degree in electrical and computer eEngineering from the same university in 2013. He obtained his Bachelor's and Master's degrees in computer science from Shanghai Jiao Tong University, China, in 2006 and 2009. His research interests include information and network security, privacy preservation, and applied cryptography for e-healthcare systems and mobile social networks.

Xiaodong Lin [S'07, M'09] (xiaodong.lin@uoit.ca) received his Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, China, in 1998 and another Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and comput-

er engineering from the University of Waterloo in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Canada. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing. He was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks (ICCCN 2009), the 5th International Conference on Body Area Networks (BodyNets 2010), and IEEE ICC 2007.

KUAN ZHANG (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 in the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include packet forwarding, and security and privacy for mobile social networks.

XUEMIN SHEN [M'97, SM'02, F'09] (xshen@bbcr.uwaterloo.ca) received his B.Sc.(1982) degree from Dalian Maritime University, China, and his M.Sc. (1987) and Ph.D. (1990) degrees from Rutgers University, New Jersey, all in electrical engineering. He 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, wireless body area networks, and vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering. He has served as the Technical Program Committee Chair for IEEE VTC '10 Fall, Symposia Chair for IEEE ICC '10, Tutorial Chair for IEEE VTC '11 Spring and IEEE ICC '08, Technical Program Committee Chair for IEEE GLOBECOM '07, General Co-Chair for Chinacom '07 and QShine '06, Chair for IEEE Communications Society's Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as Editor-in-Chief for *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*; a Founding Area Editor for *IEEE Transactions on Wireless Communications*; an Associate Editor for *IEEE Transactions on Vehicular Technology*, *Computer Networks*, and *ACM/Wireless Networks*; and as a Guest Editor for *IEEE JSAC*, *IEEE Wireless Communications*, *IEEE Communications Magazine*, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. 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 the IEEE Vehicular Technology and Communications Societies. He has been a guest professor of Tsinghua University, Shanghai Jiao Tong University, Zhejiang University, Beijing Jiao Tong University, Northeast University, and others.