SECURITY AND PRIVACY FOR MOBILE HEALTHCARE NETWORKS: FROM A QUALITY OF PROTECTION PERSPECTIVE

KUAN ZHANG, KAN YANG, XIAOHUI LIANG, ZHOU SU, XUEMIN (SHERMAN) SHEN, AND HENRY H. LUO

ABSTRACT

With the flourishing of multi-functional wearable devices and the widespread use of smartphones, MHN becomes a promising paradigm of ubiquitous healthcare to continuously monitor our health conditions, remotely diagnose phenomena, and share health information in real time. However, MHNs raise critical security and privacy issues, since highly sensitive health information is collected, and users have diverse security and privacy requirements about such information. In this article, we investigate security and privacy protection in MHNs from the perspective of QoP, which offers users adjustable security protections at fine-grained levels. Specifically, we first introduce the architecture of MHN, and point out the security and privacy challenges from the perspective of QoP. We then present some countermeasures for security and privacy protection in MHNs, including privacy-preserving health data aggregation, secure health data processing, and misbehavior detection. Finally, we discuss some open problems and pose future research directions in MHNs.

INTRODUCTION

Healthcare is one of the major social and economic problems around the world, especially in an aging society, where it entails tremendous health expense and labor resources. From a recent national health report in the United States, the average expense per capita was $8895 in 2014, while the annual national healthcare expenditure has skyrocketed to $3.8 trillion. Among the costs, nursing home care, home health care, and personal care contribute about 18 percent of the total expenditure [1]. Moreover, traditional hospital-centric healthcare not only lacks efficiency when dealing with chronic diseases or identifying some serious diseases in the early stages, but also suffers from excessive waiting times in hospitals. Therefore, it is emerging to pose up-and-coming healthcare solutions, including continuous health monitoring as well as health information processing and sharing, to enhance disease diagnosis and release the heavy burden of the existing health expenditure.

Recently, wearable devices (e.g., smart wristwatches, bracelets, rings, and hair caps) are widely applied to offer continuous healthcare, such as physiology parameter monitoring for remote healthcare [2], heart rate recording for workout intensity or training, and calorie burn during fitness. Consisting of these ubiquitous wearable devices, heterogeneous mobile networks (e.g., cellular network, WiFi, and device-to-device [D2D] communications), and powerful computational servers (e.g., cloud servers), mobile healthcare networks (MHNs) collect the health information sensed by wearable devices, analyze/process for health monitoring and diagnosis, and enable users' social interactions. For example, seniors can wear dedicated wearable devices that continuously measure their physiology information, such as body temperature, heart rate, blood pressure, and oxygen saturation. Meanwhile, doctors and/or their families can use desktops and smartphones to remotely access these health records via MHNs. In case of any emergency, such as falling down or a heart problem, the wearable devices can automatically report the health condition of the patient to his/her doctors and families. In addition, MHNs can also enable promising wearable and social applications, for example, sharing physical condition and activity information measured by wearable devices among social friends [3].

However, MHN applications raise various security and privacy issues. Since health information (e.g., phenomena, health condition, emergency) is relatively sensitive for users, any inappropriate disclosure may violate user privacy and even result in property loss [2]. Users may also worry about their critical health data being tampered with when their health data are stored in untrusted cloud servers [4]. Moreover, some malicious attackers misbehave in MHNs to disrupt the effectiveness or mislead other users'

Kuan Zhang, Kan Yang, and Xuemin (Sherman) Shen are with the University of Waterloo.

Xiaohui Liang is with Dartmouth College.

Zhou Su is with Waseda University.

Henry H. Luo is with Care In Motion (CIM) Technology Inc.

1536-1284/15/$25.00 © 2015 IEEE

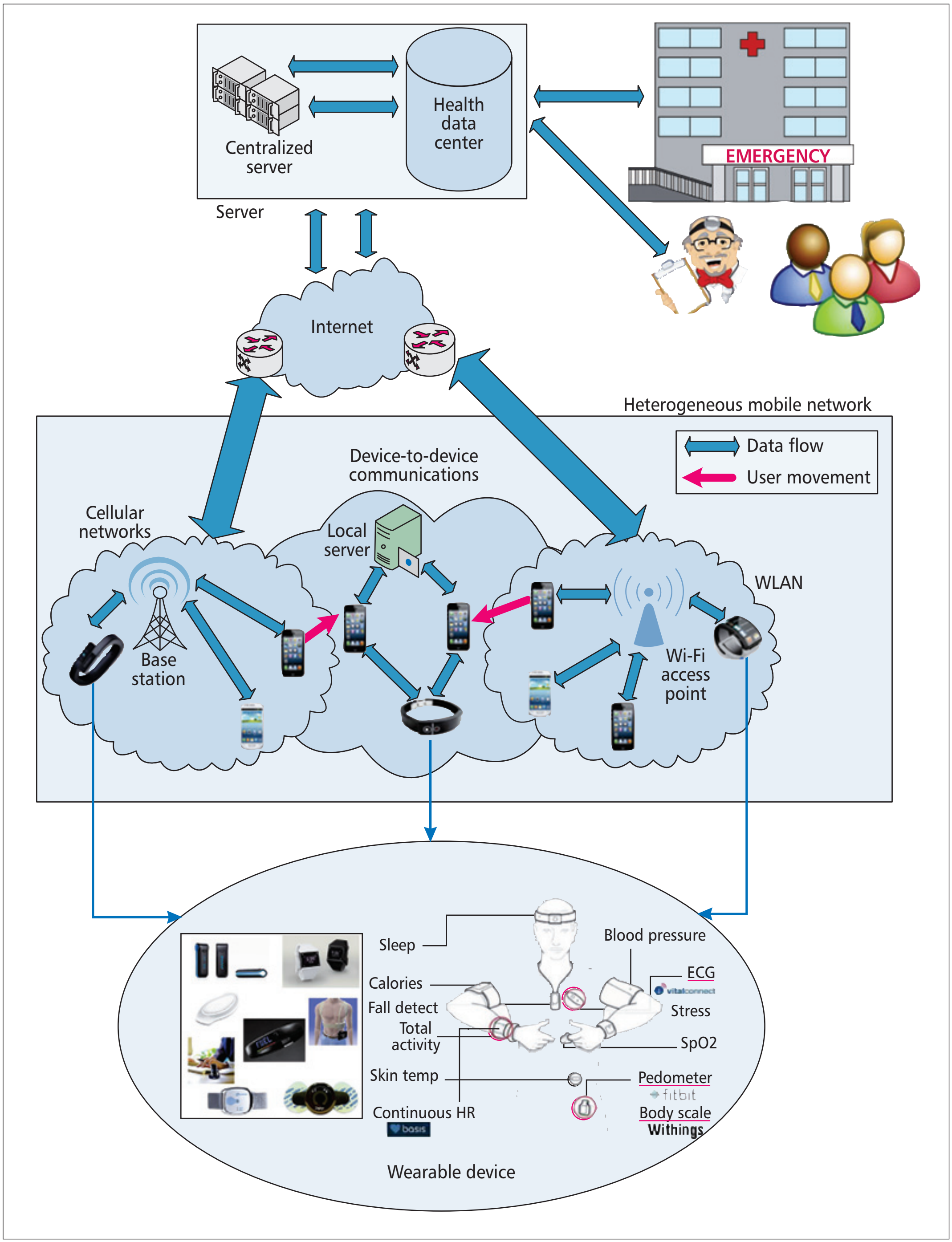


Figure 1. Mobile healthcare network.

To satisfy users' diverse security requirements and balance the trade-off between the performance and security protections, quality of protection QoP has become a newly emerging security concept that allows applications to seamlessly integrate adjustable security protection.

preferences [5]. Without appropriate security and privacy protections, users may not accept MHN applications.

In addition, the costs of security protections vary with users' diverse demands, and may impact users' experiences of MHN applications. For example, complicated encryption techniques may offer users more security guarantees but with higher computational overheads and latency than lightweight ones. To satisfy users' diverse security requirements and balance the trade-off between the performance and security protections, quality of protection (QoP) has become a newly emerging security concept that allows applications to seamlessly integrate adjustable security protection [6, 7]. Therefore, we shine a special spotlight covering MHN trends in security and privacy protection from the QoP perspective, which can separate security schemes into different levels to ensure the suitable security services for the best trade-off between performance demands and security.

In this article, we investigate security and privacy issues in MHNs from the QoP perspective. We first introduce the overall architecture of MHNs, and present some promising MHN applications. Then we discuss the security and privacy challenges in MHNs from the QoP perspective,

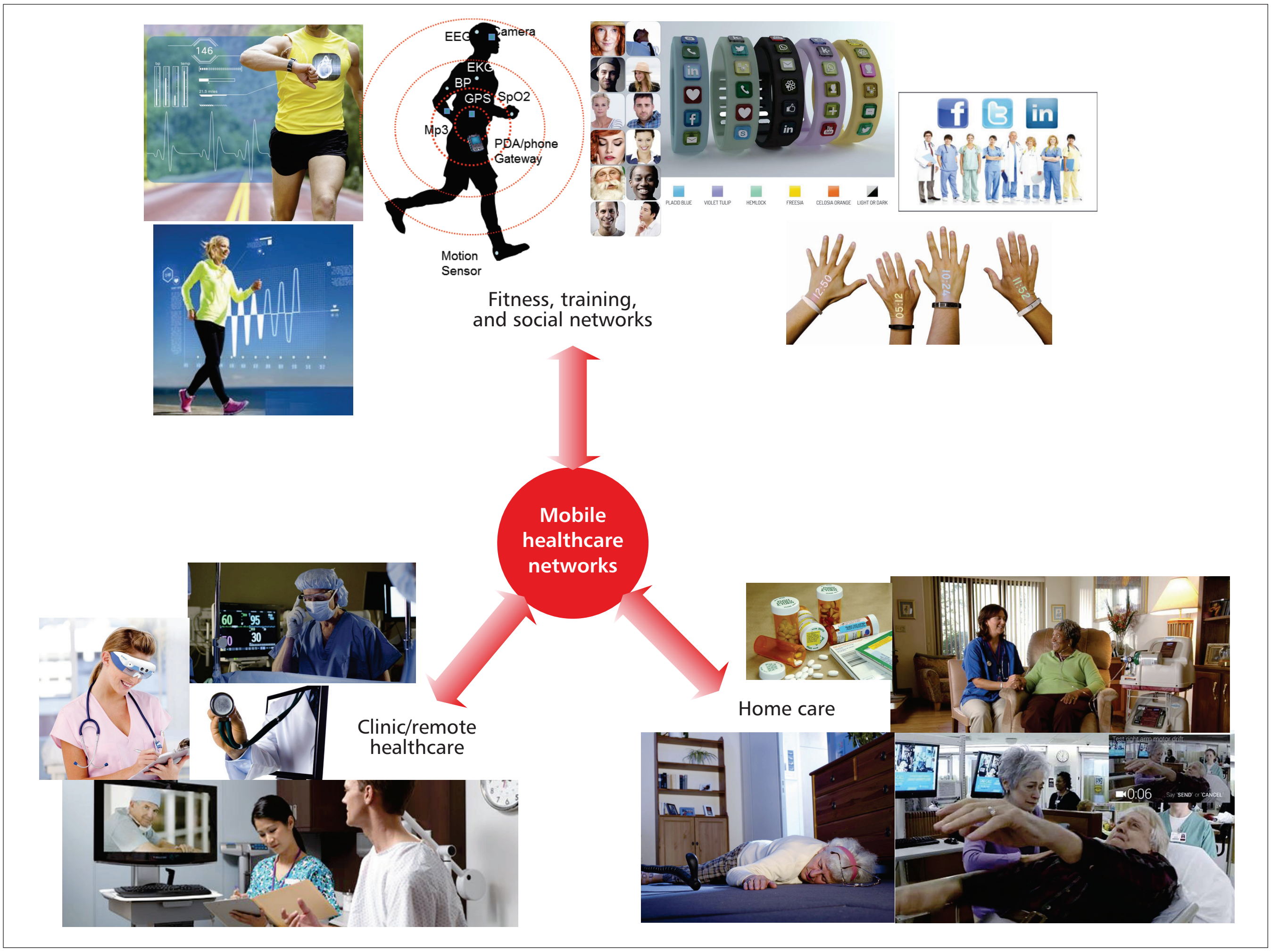


Figure 2. MHN applications.

including privacy leakage, misbehavior, and security in health data collection and processing. We also present some solutions, that is, privacy-preserving health data aggregation, misbehavior detection, and secure health data processing, to address these security and privacy challenges. Finally, we present some open problems and indicate future research directions.

MHN Architecture and Applications

In this section, we present the heterogeneous MHN architecture and introduce some promising MHN applications.

MHN Architecture

MHNs consist of wearable devices, users, servers, and heterogenous mobile networks as shown in Fig. 1.

Wearable Devices: Wearable devices, as the bridge connecting the human body and information world, are integrated with physiology sensors, and low-power computation, communication, and storage modules. These devices can sense diverse information from a human, such as physiology parameters, health conditions, motions, and location. Generally, wearable devices can only preprocess the sensed data due to the limitations of size, processing capabilities, and energy. Alternatively, these sensed data are compressed by the embedded low-power computation modules, sent to mobile users' devices (i.e., smartphones and desktops) via Bluetooth or NFC, or directly delivered to the servers via heterogeneous mobile networks.

Users: Users, such as doctors, patients, and their families, use smartphones to receive sensing data from wearable devices. They can also deliver these health data to servers for further processing and analysis. Furthermore, they can be either sensing objects (e.g., patients and seniors) of wearable devices or monitors to measure and collect health data from the sensing objects.

Servers: The servers (e.g., centralized servers in hospitals and cloud servers) are used to store, process, and analyze the collected health data from the wearable devices or mobile users. Some local servers can perform as authorities to automatically organize the local MHNs and provide local information to facilitate mobile users' interactions.

Heterogeneous Mobile Networks: Consisting of cellular network, WiFi, and D2D communications, heterogeneous mobile networks support MHNs for health data collection from wearable devices or mobile users, transmission, and shar-

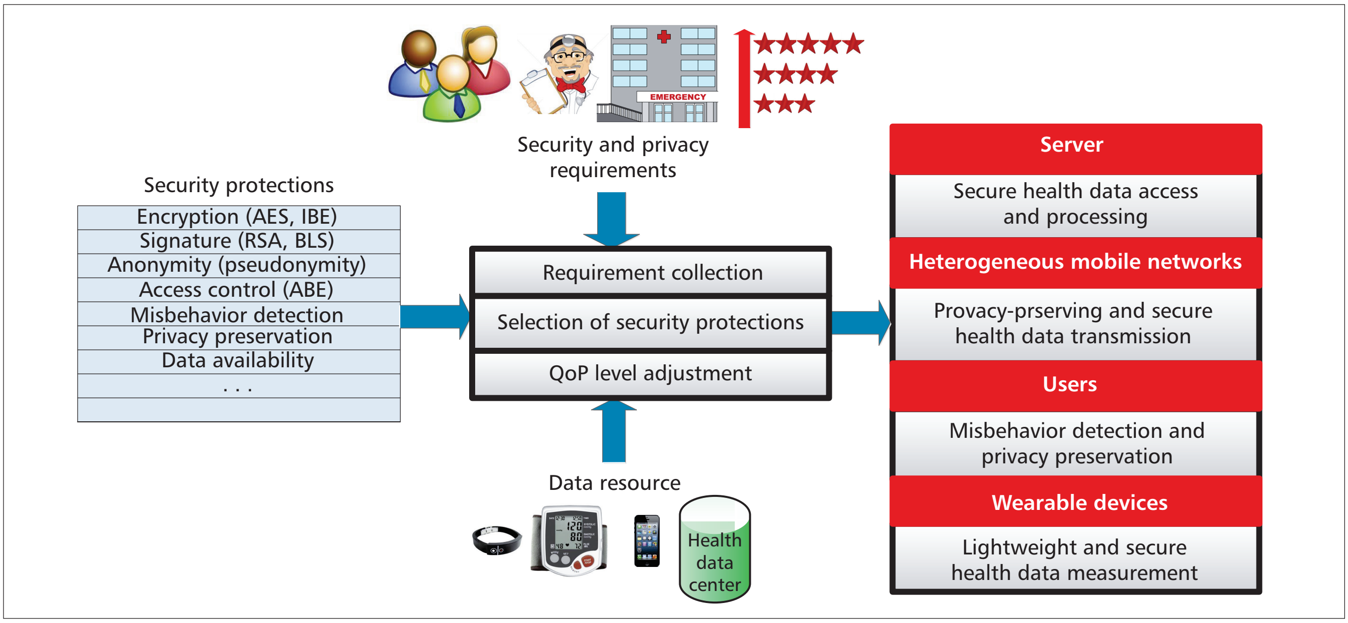


Figure 3. QoP in MHNs.

ing. MHNs can be switched seamlessly among different types of mobile networks during health data transmission and sharing. With heterogeneous mobile networks, mobile users can access the Internet through WiFi or cellular networks, interact with surrounding users via Bluetooth or NFC, and browse local information via local servers.

MHN Applications

There are various MHN applications, including remote healthcare, home care, and fitness, as shown in Fig. 2.

Clinic/Remote Healthcare: Health monitoring is one of the most prestigious MHN applications, offering continuous physiology parameter sensing, health condition monitoring, and so on. The multi-functional wearable devices can measure various physiology and activity parameters, such as heart rate, body temperature, blood pressure, oxygen saturation, blood volume index, respiration, pulse, quality of sleep, location, falls, and posture. Doctors and related family members can remotely and in real time check the health condition of the patients, or diagnose a chronic disease at an early stage.

Home Care: Home care can offer ubiquitous healthcare for seniors and disabled people, even though they stay at home, which considerably saves hospital resources with convenience for patients. Fall detection is a typical emergency response application in MHNs, where the abnormal body position can trigger acceleration sensors to identify the fall, and wearable devices or smartphones can report this emergency to the patient's family and doctors through MHNs. Furthermore, the real-time physiology parameters can be measured after the fall, offering a guideline for emergency operation.

Fitness and Training: Despite the aforementioned health monitoring related applications, MHNs can also offer a wide range of applications, including fitness and training. The wearable devices (e.g., belt, glove, and bracelet) are able to capture the motion of the human body, arms, or hands, measuring calorie burn and heart or lung conditions during fitness and training. The sensed health data become the main driver of users' further fitness plan or the coach's decisions. During workouts, users can also share their physiology parameters with each other for experience sharing or feedback [8]. For example, they can share suitable fitness guidelines with users having similar physical conditions, or recommend health products (e.g., protein and healthy foods).

Security and Privacy Issues in MHNs from a QoP Perspective

With the main drivers of user experience [9] and security service requirements, QoP is becoming an important security concept to provide different levels of security protection to different levels of users with diverse demands. Specifically, as shown in Fig. 3, MHNs with QoP can achieve access privileges via authentication; guarantee integrity, confidentiality, and non-repudiation via encryption and signature; ensure copyrights via watermarking; and protect privacy via cryptography, anonymity, and obfuscation techniques [9]. Having a set of security protection services, QoP, fueled by artifacts, human intelligence, and involvement, adjusts these tunable protection aspects according to different requirements. Besides these off-the-shelf security protection schemes applied in QoP, several other emerging approaches to dealing with the critical security and privacy issues in MHNs are also essential from the QoP perspective.

Privacy Leakage

Privacy is a critical issue in MHNs as sensitive health data are involved in collection, transmission, processing, and sharing. Without appropri-

As MHNs may take advantage of the powerful storage and computation capabilities of outsourced cloud servers, security concerns associated with these untrusted cloud servers are also raised in MHNs. The health data access policy should be clearly defined and used to authenticate the user's identity with access authority.

ate privacy protection, users may not be willing to expose their data to others, which hinders the processing and sharing of health data and users' experiences. In [4], several general privacy threats in a healthcare system, such as identity privacy, information leakage during transmission, and location privacy, are investigated. In [5], privacy protection is applied between sensors and smartphones to protect against sensing data disclosure. In [6], Ong *et al.* investigate security services partitioned into various security levels to balance security requirements and performance preferences. A proper QoP construction can be offered by the characterization of QoP with security settings, where it expresses security constraints and attributes to customize protection for different applications. In MHNs, to achieve a higher privacy level of data and users' profiles (or attributes), for example, personal physiology parameters, the privacy protection should be robust and strong enough to resist potential attacks and leakage, which inevitably increases computational overheads and latency. Therefore, QoP should be applied in MHNs for adjusting the privacy protection at various privacy levels.

Secure Data Access and Processing

As MHNs may take advantage of the powerful storage and computation capabilities of outsourced cloud servers, security concerns associated with these untrusted cloud servers are also raised in MHNs. The health data access policy should be clearly defined and used to authenticate the user's identity with access authority. For example, for a patient's daily health data (e.g., electrocardiography [ECG]) stored in the cloud server, only the doctors in neurology can access these data and the corresponding analysis results. Meanwhile, the data should be protected from being accessed by an insurance company [10]. Besides the general access control policies, it is also critical to ensure fine-grained access in accordance to users' attributes. In MHNs, dynamic access management is necessary to address the issues of users' attributes changing, revocation, a new user's participation, and so on. In addition, the overheads for different access levels should be balanced to release the computation burden for users.

When health data are outsourced to cloud servers for analysis and processing, the raw data should be invisible to the untrusted cloud servers, and the user's (e.g., data owner's) identity and associated profiles should be anonymous. Some secure health data processing schemes (e.g., functional encryption, homomorphic encryption) are proposed to guarantee data protection during some basic operations (e.g., aggregation, summation, and comparison). With different QoP requirements, the protection should be enhanced when applying some complicated operations, such as Bayesian learning and data mining, which are essential for health data analysis and diagnosis.

Malicious Attacks and Misbehavior

MHNs are vulnerable to malicious attacks and misbehavior from mobile users, which may disrupt the effectiveness of MHNs or degrade the performance. In health-related social applications, such as fitness and social gaming, attackers may forge their social attributes to snatch other legitimate users' health information, leading them to push some spam recommendations and violate users' privacy. Moreover, these attackers may also misbehave, for example, not following the network protocol or spreading spam to launch denial of service (DoS) attacks or consuming a large amount of network resources. Although some misbehavior detection schemes [4] can partially resist individual attacks, it is still challenging to adjust the security protection against powerful attacks such as Sybil attacks. The cost of misbehavior detection may increase due to the skyrocketing attacking capabilities of these attackers. To offer MHNs from the QoP perspective, the misbehavior should be categorized into different levels with the corresponding detection or protection schemes.

Security Solutions in MHNs

In this section, we present some security solutions for the emerging MHN applications from the perspective of QoP.

Privacy-Preserving Health Data Aggregation

In MHNs, the data transmission (or forwarding) overheads are exponentially increased due to the large number of health sensing data from wearable devices. Particularly, in a D2D-based smart community as shown in Fig. 4, users continuously upload their physiology parameter records to a health data center via social spots deployed in the community by using short-range communication techniques. Furthermore, the multihop relay is adopted to aggregate the data with a tolerable delay. However, in accordance with different types of health data, the transmission delay may be significantly different. Meanwhile, privacy protection during data transmission is also necessary for MHNs.

In [11], a priority-based privacy-preserving data aggregation scheme is proposed for MHNs, which not only aggregates different types of health data within tunable delay requirements but also protects the data and identity privacy during transmission. According to various types of health data, users select different forwarding strategies, which not only forward data within the given delay but also consume reasonable network resources. Having the health data priority shown in Fig. 4b, users with P1 data can greedily forward their data and make use of the network resources to minimize the delay. Furthermore, doctors may request vital health data from patients in emergencies for continuous monitoring. In addition, the regular health data are not for emergency use, so the delay requirement may be tolerant. Both vital and regular data are labeled as small data (i.e., physiology parameters with small data size) and big data (i.e., ECG or images with large size) [11]. Given the relay selection strategy, the sender selects the optimal relay for different data priorities (or different forwarding schemes). Then the relays store-carry-and-forward the data to social spots connected to cloud servers so that the data can finally be forwarded to the cloud servers.

The security and privacy issues cannot be negligible as the cloud servers are not fully trusted and may maliciously delete or modify the stored data. Moreover, the data owner cannot trust the relays who are anonymous and even strangers. Since the health data are separated into different categories, the security protection levels should also be adjusted. Therefore, to enhance the health data aggregation from the QoP perspective, privacy-preserving aggregation is desirable.

In [11], a superincreasing sequence is adopted to separate different priorities of health data. If the amount of data and the maximum data value in each priority from N users are smaller than constant ϕ and θ, the trusted authority (TA) can generate a superincreasing sequence $\vec{b} = (b_1 = 1, \dots, b_N)$ with each element denoting a large prime, where $\Sigma_{j=1}^{i-1} b_j \cdot \phi \cdot \theta < b_i$ for $i = 2, \cdots, N$, and $\Sigma_{j=1}^{n} b_j \cdot \phi \cdot \theta < n$. To differentiate the encrypted data for each type, the TA generates the other superincreasing sequence $\vec{a} = (a_1 = 1, a_2, a_3, a_4, a_5)$, where a_2, a_3, a_4, and a_5 are all large primes. Here, $\Sigma_{j=1}^{i-1} a_j \cdot \gamma \cdot \theta < a_i$ for $i = 2, \cdots, 5$, and $\Sigma_{j=1}^{5} a_j \cdot \gamma \cdot \theta < n$, where $\Sigma_{j=1}^{n} b_i = \gamma$. The TA also has $g_i = g^{a_i}$ for $i = 1, 2, \cdots, 5$ and constructs $(g_1, g_2, \cdots, g^5)$. The secret keys are $\{\lambda, \mu, \vec{a}, \vec{b}\}$, while the public keys are $\{n, g\}$.

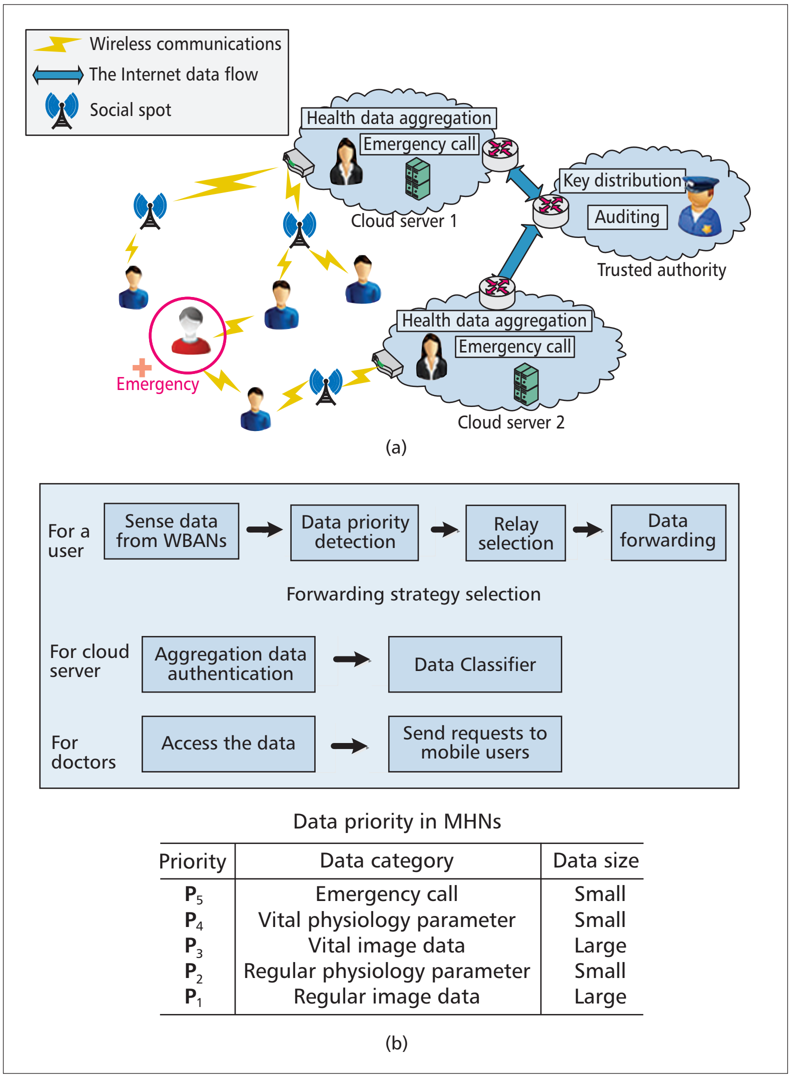
During initialization, an individual user u_i receives his/her secret keys b_i from the TA. Having the pseudonym techniques, u_i is also assigned a set of asymmetric key pairs and generates the pseudonym PID$_i$ during the communications. The unique identity u_i can be protected since only the literally meaningless pseudonyms are visible to others. When the data $(d_1, d_2, d_3, d_4, d_5)$ are monitored and separated into different priorities (from P1 to P5), u_i encypts the data as $C_{i,j} = g_j^{b_i d_{i,j}} \cdot r_i^n \bmod n^2$, where $j \in \{1, 2, 3, 4, 5\}$ is the priority number and $r_i \in Z_q^*$ is a random number. The aggregated ciphertext is

$$C = \prod_{j=1}^{5} g_j^{\sum_{i=1}^{N} b_i d_{i,j}} \left(\prod_{i=1}^{N} r_i\right)^n \bmod n^2 .$$

Having the secret key (λ, μ), the ciphertext C can be decrypted as $M = (a_1 \Sigma_{i=1}^{N} b_i d_{i1} + a_2 \Sigma_{i=1}^{N} b_i d_{i2} + \dots + a_5 \Sigma_{i=1}^{N} b_i d_{i5}) \bmod n$. The raw data $(d_1, d_2, d_3, d_4, d_5)$ can be obtained by using a recursive algorithm based on the features of a super-increasing sequence. Therefore, the data are privately aggregated at different priorities with the corresponding service requirements, where users' experiences and privacy are balanced with tunable QoP provisioning.

Secure Health Data Access and Processing

Health data access, processing, and analysis are of utmost importance during healthcare management, health condition analysis, and diagnosis. It is necessary to confine the health data access in the server and prevent raw data disclosure during the processing procedures. In [12], a normalized weighted tree is adopted to describe the security system attributes, where the elements of the security system structure are identified as nodes of the tree. By expanding/shrinking the tree, these security system attributes can be represented to permit the definition, formulation, and evaluation for model-based QoP. Therefore, QoP is an extension of the current QoS model on security protection.



Data priority in MHNs

Priority	Data category	Data size
P_5	Emergency call	Small
P_4	Vital physiology parameter	Small
P_3	Vital image data	Large
P_2	Regular physiology parameter	Small
P_1	Regular image data	Large

Figure 4. Priority-based health data aggregation for MHNs: a) cloud assisted WBAN model; b) priority-based health data aggregation.

Authentication is the first step to enable legal users (e.g., with valid signature or certificate) from outside to access the data. But the raw data are still visible to the untrusted cloud servers [13]. Alternatively, the raw data can be encrypted and stored in the cloud servers so that only the users having the decryption keys can access the raw data. As such, the data are selectively visible at a coarse-grained access, that is, providing others the decryption keys. Meanwhile, it resists the cloud servers' efforts to process the data, which hinders the cloud server's advantages of data processing and limits the flourishing of MHNs. To achieve the fine-grained access control, attribute-based encryption (ABE) has evolved in the past decades to improve the flexibility in specifying differential data access [14]. Every user maintains a set of descriptive attributes associated with his secret keys, while the ciphertexts are labeled with the defined access policy. As a result, only autho-

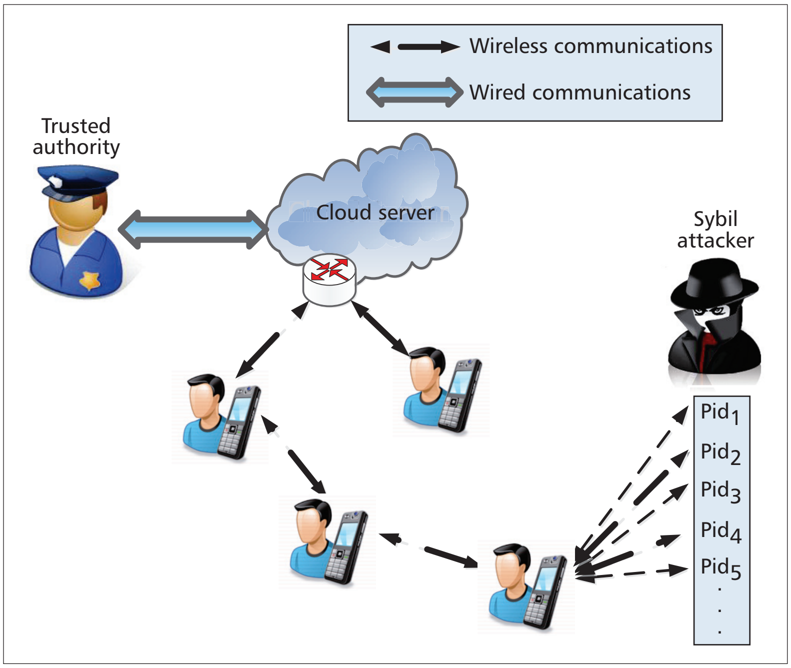


Figure 5. Sybil detection for MHNs.

rized users with specific attributes satisfying the access policy can decrypt the raw data.

In terms of health data processing, the computational operations in the cloud server pose challenges since the data are generally encrypted without access authorization for the untrusted cloud servers. To this end, some enhanced cryptographic schemes are adopted toward some specific operations, for example, homomorphic encryption for summation and multiplication, searchable encryption for search, predicate encryption, order-preserving encryption, hidden vector encryption for query and comparison, and so on. In addition, the recent functional encryption also achieves the similar objectives of data processing. Although these cryptographic schemes allow the cloud servers to perform some basic computational operations over the encrypted data and preserve data privacy, it is still necessary to develop efficient approaches to the complicated and diverse operations for MHNs from the perspective of QoP.

Misbehavior Detection for Health-Oriented Mobile Social Network Application

MHNs offer users a wide range of social network applications, such as fitness experience sharing, health data exchange, and instant interaction among social friends. However, some attackers may not honestly follow the network protocols and even misbehave to not only degrade the MHN performance and users' experiences but also disrupt MHNs. A Sybil attack is one of these serious threats to MHNs, where Sybil attackers maliciously manipulate a large number of pseudonyms (or identities) to cheat others. For example, during fitness experience sharing in MHNs, Sybil attackers may repeatedly send the same fitness experiences to the same users with multiple identities to mislead other users' opinions and preferences, as shown in Fig. 5. Furthermore, it is difficult to trace Sybil attackers in MHNs due to the unpredictable trajectories and high mobility, which poses a new set of challenges and requires urgent solutions to detect them.

Generally, Sybil attacks in large-scale networks can be detected with social graph or community detection, or utilize cryptography to detect Sybil attackers. However, mobile users cannot easily detect Sybil attackers in mobile environments due to some limitations:

- There are weak social relationships since mobile users sometimes may not have tight social relationships with others in physical proximity.
- Dynamic user mobility results in intermittent social connections.
- Smarter Sybil attackers usually act similar to normal users, which leads to merging into normal users' social communities and lowering resistance to traditional detection.
- There are limited knowledge and detection capabilities.

One of the promising solutions is to take the advantage of the cloud server in MHNs for the detection. As security concerns are introduced by the cloud server, it is still tricky to find a thorough Sybil detection approach in MHNs from the perspective of QoP.

To this end, in [15], a social-based mobile Sybil detection scheme is proposed, which explores mobile users' pseudonym changing behaviors and contact statistics to differentiate Sybil attackers from normal users.

With the increasing attack capabilities, Sybil attackers can be defined in four levels.

L-1: *General Sybil attackers* adopt pseudonyms to hide their real identities (through frequently changing pseudonyms) and repeatedly send the similar information or spam to normal user u_i. From u_i's view, the received information seems to be from different users, so u_i's preference may be biased.

L-2: *Sybil attackers with forged contact* can forge some fake contact records (without contact signatures) with other users to confuse Sybil detection. In other words, a large number of fake contact records can support an L-2 attacker's pseudonym change.

L-3: *Sybil attackers with mobile users' collusion* provide nonexistent contact records with valid contact signatures, even though the colluding users have not met each other.

L-4: *Sybil attackers with collusion of cloud servers* either add some fake contact records for attackers to help validate their pseudonym changing, or modify and delete normal users' contact records to increase the false detection rate.

In [7], Luo *et al.*, propose a QoP partition model that quantitatively reflects strength of protection and users' security demands. To provide QoP toward these levels of Sybil attacks in MHNs, in [15], the corresponding countermeasures are proposed as follows.

C-1: Each mobile user provides the contact records associated with his/her pseudonym change. If a pseudonym is changed when the number of contacts is below a threshold *TH*, L-1 attackers can be detected.

C-2: Mobile users collect the contact signa-

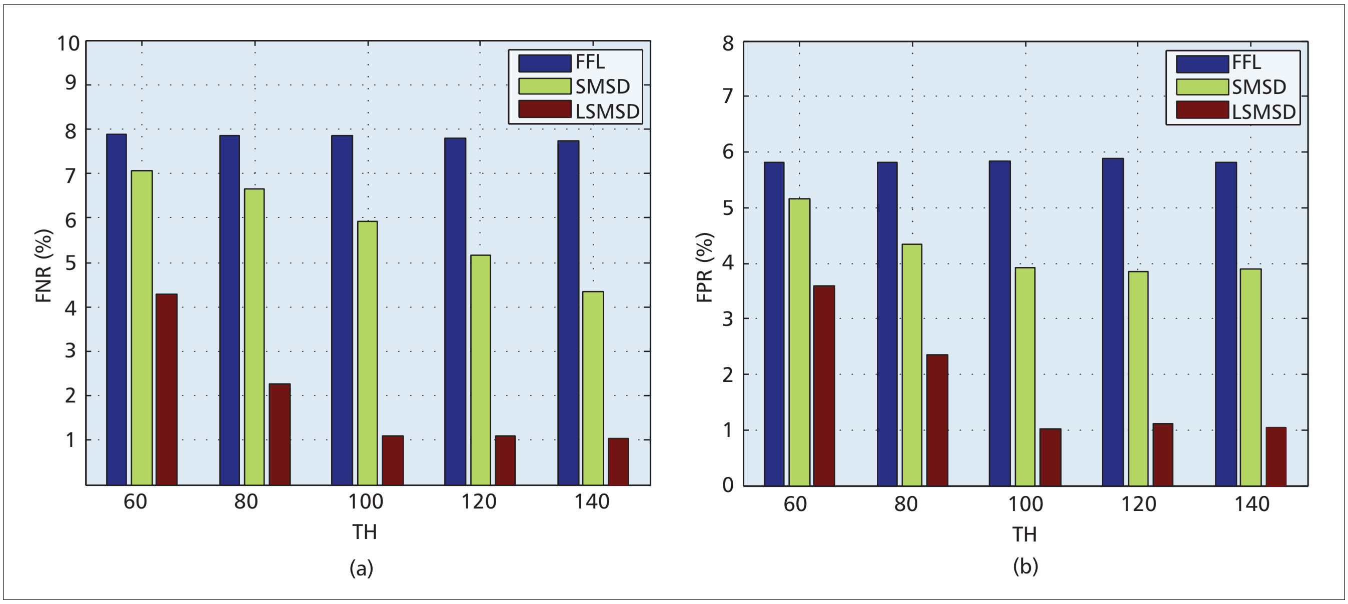


Figure 6. Performance comparison of mobile Sybil detection (TH is the threshold to change pseudonyms: a) FNR vs. TH; b) FPR vs. TH.

ture of each encountered user. As evidence of the contact, the contact signature is generated by each pair of the encountered legitimate mobile users. A variant of the aggregate signature technique is proposed to reduce the overall signature size and verification overhead.

C-3: If a user has a dramatically high volume of contacts with a specific user while having only a few contacts with other users, it is suspicious and likely to be collusion. Based on the observation of normal users' contact rate distribution, a semi-supervised learning with a hidden Markov model (HMM) is proposed to differentiate the abnormal contact rates that are likely from colluded users. With social proximity estimation, the collusion can be detected based on the learning results. The proposed learning scheme can balance the overhead of ground-truth data training and the detection accuracy since it is adaptive to abnormal states.

C-4: Before uploading the contact records to untrusted cloud servers, each mobile user should form the contact signatures in a specific structure (e.g., chain or ring) in which each item cannot be removed or modified by a third party. The contact signatures form a closed ring structure, while the established bidirectional hash chains guarantee the order of each contact time. A contact list is synchronized with the contact order list by the users to validate the integrity of the contact records in the cloud servers.

We adopt false negative rate (FNR) and false positive rate (FPR) to evaluate the Sybil detection performance, as shown in Fig. 6. Toward different levels of Sybil attacks, MHNs are able to adjust the tunable detection strategies from the perspective of QoP.

Conclusion and Outlook

In this article, we have introduced the MHN architecture and identified the security and privacy requirements from the perspective of QoP. Furthermore, we have provided information on some emerging MHN applications associated with the challenging security and privacy issues. From the QoP perspective, we have presented the security countermeasures, which can be adjusted to satisfy MHN users' diverse requirements about service, experience, and protection.

However, there are also a set of immature security and privacy solutions for MHNs without consideration of QoP. First, although current wearable devices can offer diverse functionalities to sense multiple physiology parameters, they still lack lightweight security protection. Due to the low power and portability of these wearable devices, the traditional cryptographic schemes may considerably increase the computation and communication overheads. Compressive sensing is a prestigious approach to integrating lightweight data sensing and security (e.g., encryption and signature) from the perspective of QoP. Having the sensing matrix, the raw data, which can be sparsely expressed in some domain (e.g., time, frequency, or wavelet), are compressed with different rates. During the construction of a sensing matrix, it is difficult to find such a matrix with low coefficient between any two columns. Therefore, it is still an open problem and requires more research effort.

Second, during health data processing in MHNs, it is urgent to allow a cloud server to perform complicated operations on the encrypted data. For example, machine learning and data mining algorithms can be applied to analyze the physiology parameters and disease. The anonymity techniques should be integrated with the cryptography schemes to balance the privacy and the health data usability. However, it is challenging to achieve the trade-off between the security and complexity of data processing, especially from the perspective of QoP.

Finally, as smarter attackers tend to mimic normal users to hide themselves against security solutions, the traditional approaches focused on resisting the attacking behavior may not be effective under some circumstances. Misbehavior detection relies on the learning procedures where learning and training are alternatively applied. Furthermore, human intelligence is highly desirable during the misbehavior modeling and detection to adjust the tunable security and privacy solutions with QoP.

Misbehavior detection relies on the learning procedures where learning and training are alternatively applied. Furthermore, human intelligence is highly desirable during the misbehavior modeling and detection to adjust the tunable security and privacy solutions with QoP.

We hope this article sheds more light on security and privacy protection for MHNs from the QoP perspective, which requires further research effort along this emerging line.

Acknowledgment

This research has been supported by a research grant from the Natural Science and Engineering Research Council (NSERC) and Care In Motion (CIM) Technology Inc., Canada.

References

[1] Forbes; available:http://www.forbes.com/

[2] X. Liang *et al*., "Enabling Pervasive Healthcare through Continuous Remote Health Monitoring," *IEEE Wireless Commun*., vol. 19, no. 6, Dec. 2012, pp. 10–18.

[3] A. Toninelli, R. Montanari, and A. Corradi, "Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks," *IEEE Wireless Commun.*, vol. 16, no. 3, June 2009, pp. 24–32, .

[4] J. Zhou *et al*., "Securing m-Healthcare Social Networks: Challenges, Countermeasures, and Future Directions," *IEEE Wireless Commun.*, vol. 20, no. 4, Aug. 2013, pp. 12–21.

[5] H. Wang *et al*., "Resource-Aware Secure ECG Healthcare Monitoring Through Body Sensor Networks," *IEEE Wireless Commun*., vol. 17, no. 1, Feb. 2010, pp. 12–19.

[6] C. Ong, K. Nahrstedt, and W. Yuan, "Quality of Protection for Mobile Multimedia Applications," *Proc. IEEE ICME*, 2003, pp. 137–40.

[7] A. Luo *et al*., "Quality of Protection Analysis and Performance Modeling in IP Multimedia Subsystem," *Computer Commun*., vol. 32, no. 11, July 2009, pp. 1336–45.

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

[9] M. Katsarakis *et al*., "On User-Centric Tools for QoE-Based Recommendation and Real-Time Analysis of Large-Scale Markets," *IEEE Commun. Mag.*, vol. 52, no. 9, Sept. 2014, pp. 37–43.

[10] M. Barni *et al.*, "Privacy-Preserving ECG Classification with Branching Programs and Neural Networks," *IEEE Trans. Info. Forensics Security*, vol. 6, no. 2, Jan. 2011, pp. 452–68.

[11] K. Zhang *et al*., "PHDA: A Priority Based Health Data Aggregation with Privacy Preservation for Cloud Assisted WBANs," *Elsevier Info. Sciences*, vol. 284, Nov. 2014, pp. 130–41.

[12] Y. Sun and A. Kumar, "Quality-of-Protection (QoP): A Quantitative Methodology to Grade Security Services," *Proc. IEEE ICDCS*, 2008, pp. 394–99.

[13] H. Lin *et al*., "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," *IEEE Trans. Info. Forensics Security*, vol. 8, no. 6, Mar. 2013, pp. 985–97.

[14] V. Goyal *et al*., "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. SIGSAC*, 2006, pp. 1–28.

[15] K. Zhang *et al*., "Exploiting Mobile Social Behaviors for Sybil Detection," *Proc. IEEE INFOCOM*, 2015, pp. 271–79.

Biographies

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

Kan Yang received his B. Eng. degree from the University of Science and Technology of China in 2008 and his Ph.D. degree from City University of Hong Kong in August 2013. He is currently a postdoctoral fellow with the Electrical and Computer Engineering Department of the University of Waterloo, Canada. He was a visiting scholar at the State University of New York at Buffalo in 2012. His research interests include cloud security, big data security, cloud data mining, cryptography, social networks, wireless communication and networks, distributed systems, and so on.

Xiaohui Liang [S'10] is currently working as a postdoctoral researcher at the Department of Computer Science, Dartmouth College, New Hampshire. He received his Ph.D. degree from the Department of Electrical and Computer Engineering of the University of Waterloo, and his Master's and Bachelor's degrees from the Computer Science Department of Shanghai Jiao Tong University. His research interests include security and privacy for e-healthcare systems and mobile social networks.

Zhou Su [S'03, M'06] received his B.E and M.E degrees from Xian Jiaotong University, Xi'an, China, in 1997 and 2000, and his Ph.D degree from Waseda University, Tokyo, Japan, in 2003. He was an exchange student between Waseda and Xi'an Jiaotong University from 1999 to 2000. His research interests include multimedia communication, web performance, and network traffic. He received the best paper award of International Conference Chinacom 2008, and the Funai Information Technology Award for Young Researchers in 2009. He is Chair of an interest group of IEEE ComSoc, Multimedia Communications Technical Committee, MENIG. He has also served as Co-Chair of several international conferences including IEEE CCNC 2011 WIP track, WICON 2011 Network track, IWCMC2012-Security track, and so on.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. 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 Technical Program Committee Chair/Co-Chair for IEEE INFOCOM '14, IEEE VTC-Fall '10, Symposia Chair for IEEE ICC '10, Tutorial Chair for IEEE VTC-Spring '11 and IEEE ICC '08, and Technical Program Committee Chair for IEEE GLOBECOM '07. He also serves or has servedserved 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 the IEEE Vehicular Technology and Communications Societies.

Henry H. Luo received his Ph.D. degree in biomedical engineering from the University of Sussex, Brighton, United Kingdom, in 1994. He is currently an expert reviewer with the Canadian Natural Sciences and Engineering Research Council (NSERC). He has been the president and CTO of CIM Technology Inc., Waterloo, Canada, since 2007, and a senior manager on DSP application of Unitron hearing, Canada, since 1998.