A Secure and Efficient Data Aggregation Scheme for Cloud-Assisted Wireless Body Area Network

Huaijin Liu, Yonghong Chen, Hui Tian, and Tian Wang
(Corresponding author: Huaijin Liu)

Huaqiao University, College of Computer Science and Technology
Xiamen 361021, China
(Email: lhjhqdx@163.com)
(Received Oct. 10, 2017; revised and accepted Mar. 27, 2018)

Abstract

The development of healthcare system has been greatly facilitated by the use of cloud-assisted wireless body area network (WBAN), which provides a more convenient and intelligent medical service for the users. However, how to establish a secure channel between WBAN and the cloud service and efficient transmission of WBAN data to the cloud service is a great challenge. In this paper, we propose a secure and efficient data aggregation scheme for cloud-assisted wireless body area network. First, we use the privacy homomorphism technique to encrypt the user data, so that the aggregation of data without decryption, to ensure the security and privacy of user data. Then use the base station to help users forward data to the cloud service and allow users to select the best relay node according to the proposed greedy forwarding model, improve the transmission efficiency of user data. The security analysis and experimental results show that the proposed scheme has high security and lower loss ratio, smaller delay and less energy consumption.

Keywords: Aggregation; Cloud-assisted WBAN; Privacy Homomorphism; Wireless Body Area Network

1 Introduction

Wireless body area network (WBAN) appears very promising for healthcare service system, as if can monitor the user's physiological parameters in a timely manner, leading to enhanced efficiency of medical services. Due to the limited computing and storage resources of WBAN, a cloud service to help deal with and store large amounts of user data can provide users with more reliable and intelligent healthcare services [15, 16]. However, there lies a challenge in designing cloud services to be combined with WBANs. The main challenge is how to ensure user identity and data privacy while improving the efficiency of user data transmission. On the one hand, in order to ensure the security and privacy of user data, the literature [2, 9, 13] proposes to establish secure communication between users and cloud services through bilinear mapping, reducing key management and storage overhead. The literature [5–7] proposed the use of chaotic public key cryptography to encrypt user data against external and internal attacks. However, these schemes are not suitable for WBAN with limited computing and storage capacity. In order to reduce the computation and communication overhead, the literature [3,4,12] proposed to use the time-varying human physiological signal to establish secure channel. But this method is limited to the symmetric network topology. On the other hand, in order to improve the transmission efficiency of user data, Liang *et al.* [8] proposed a privacy-preserving emergency call scheme PEC. The scheme protects the security of healthcare service system through an attribute-based ciphertext strategy and to transmit the emergency data to the cloud service by broadcasting. Although it can resist cloud service compromise attacks and reduce the transmission delay, the scheme has a large energy consumption. Chen *et al.* [1] proposed a privacy-preserving data aggregation scheme to reduce the communication overhead of the whole system. However, the scheme can not resist compromise attacks from users or cloud servers. Subsequently, Zhang *et al.* [14] proposed a priority-based data aggregation scheme PHDA for cloud-assisted WBAN. The scheme encrypts the user data through the Paillier public key cryptography and uses the base station to help the user forward data to the cloud service, reducing the delay and increasing the packet arrival rate. However, the scheme has a large computational complexity and can not resist compromise attacks. Therefore, how to protect the user data security while maintaining the efficient transmission of data on cloud assisted WBAN is still an important challenge.

In this paper, our goal is to design a secure and efficient cloud-assisted WBAN to address secure communication and efficient transmission issues. First, we propose a lightweight data aggregation scheme that encrypts data through privacy homomorphic technology, making the cloud service aggregate data without decrypting and

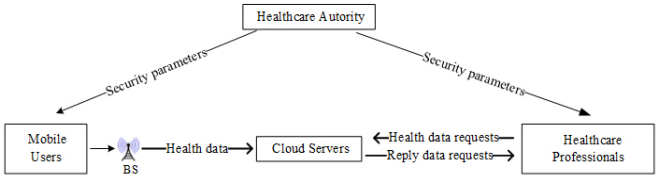


Figure 1: A generic telemedicine service architecture

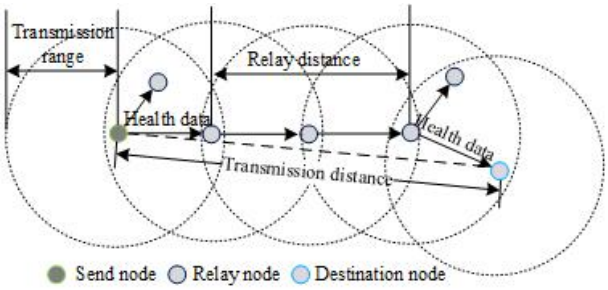


Figure 2: A greedy forwarding model

ensuring data confidentiality. Second, in order to ensure the integrity of the data, we aggregate user data labels for batch authentication, reducing the overhead of user data authentication. Finally, in order to improve the transmission efficiency of user data, we propose a greedy forwarding model to forward user data. The performance evaluation shows that our scheme can meet the requirement of delivery rate and delay, while lower energy is consumed.

2 Network Architecture and Attack Model

2.1 Network Architecture

In this section, we present a generic telemedicine service architecture, as shown in Figure 1. The architecture consists of three main components:

1) The WBAN which collects user health data;

2) The cloud service which allow medical professionals to access to stored data;

3) The healthcare authority which designate and enforce security policies.

First, the healthcare organization generates and sends his security parameters to each user and medical personnel, which is used to enforce the security policy of the medical institution. Then, WBAN collects the user's health data and uploads it to the cloud service through the base station. The cloud service to the user's data aggregation, storage and delivery to the medical personnel for diagnosis and analysis.

2.2 Greedy Forwarding Model

In WBAN, we need to consider the low power requirements of the user equipment. When the user equipment and the base station communication distance is relatively large, the use of multi-hop relay mode can reduce the total power consumption of WBAN. Then, in order to reduce the number of hops between the user equipment and the base station, we present a greedy forwarding model, as shown in Figure 2. In this model, the sending node selects the node closest to the destination node in the communication range as the next hop forwarding node.

2.3 Attack Model

Attackers may exist in the network and launched attacks to threaten the user's identity and privacy data, reduce network performance. In addition to eavesdropping, intercepting all network transmission messages, it is possible to replay the previous legitimate messages or fake legitimate users to send false messages to the base station. In addition, the user equipment and the base station are semi-trusted, and attackers are likely to launch a compromise attack on base stations and user equipment, access to the corresponding secret information to cause a greater threat.

3 The Proposed Scheme

In this section, we present a secure and efficient data aggregation scheme (SEDA). SEDA involves privacy homology [10] basic technology, in order to facilitate the later description, we first briefly introduce it.

3.1 Basic Technology

Privacy homomorphic technology does not require the aggregator to decrypt the received privacy data and can directly perform the aggregation operation. Its main principle is: take a small integer $d \geq 2$ and a large integer g as the public key, take a small divisor $g^{'}$ of g and $r \epsilon Z_g$ as the secret key; Randomly divide the message m into d parts $m_1, \cdots, m_d$, satisfy $m = \sum_{i=1}^{d} m_i mod g^{'}$, compute $E_k(m) = (m_1 r mod g, m_2 r^2 mod g, \cdots, m_d r^d mod g)$; Compute the $i-th$ coordinate by $r^{-i} mod g$ to obtain $m_i mod g$, and compute $D_k(m) = \sum_{i=1}^{d} m_i mod g^{'}$ restore m.

3.2 SEAD Scheme

This scheme is divided into four phases: initialization phase, data encryption phase, data aggregation phase and data decryption phase. The verification work is carried out in the data decryption phase.

3.2.1 Initialization Phase

The healthcare authority TA first selects a positive integer $d \geq 2$ and a large integer g as the public key,

and selects a small divisor $g^{'}$ of g and $r \epsilon Z_g$ as the private key. Then randomly generates a shared key SK_i for each user u_i and selects two one-way function: $H_1 : \{0,1\}^* \times Z_g \rightarrow Z_g$, $H_2 : Z_g \rightarrow Z_g$. Finally, TA preloads $\left\{r, g^{'}, SK_i, H_1, H_2\right\}$ into u_i.

3.2.2 Data Encryption Phase

The user u_i needs to encrypt m_i before uploading the physiological data m_i to base station BS. Before u_i encrypts, first it needs to calculate seed mask value $r_i^1 = H_1\left(ID_{u_i} \parallel SK_i\right)$, and then calculate $r_i^u = H_2\left(r_i^{u-1}\right)$ before each encryption. Using the seed mask value r_i^u to mask the encrypted data m_i : $\widehat{m}_i = \left(m_i + r_i^u\right) modg$, and then divide $\widehat{m}_i$ into d part $m_{i1}, \cdots, m_{id}$, satisfy $\widehat{m}_i = \sum_{j=1}^{d} m_{ij} modg^{'}$. Calculate C_i:

$$\begin{aligned} C_i &= [C_{i1}, C_{i2}, \cdots, C_{id}] \\ &= \left[m_{i1} r modg, m_{i2} r^2 modg, \cdots, m_{id} r^d modg\right] \end{aligned} \tag{1}$$

and calculate the label $dgt_i^u = \left(r_i^u + sk_i\right) modg$. Then forwards $C_i \parallel dgt_i^u$ to the nearby BS through the greedy forwarding model.

3.2.3 Data Aggregation Phase

When the cloud service receives the n messages sent by BS in the time period t, it needs to aggregate the n messages:

$$\begin{aligned} C_{12\cdots n} = & \sum_{i=1}^{n} C_i = \left[\sum_{i=1}^{n} C_{i1}, \cdots, \sum_{i=1}^{n} C_{id}\right] \\ = & \left[\sum_{i=1}^{n} m_{i1} r modg, \cdots, \sum_{i=1}^{n} m_{id} r^d modg\right] \end{aligned} \tag{2}$$

$$Dgt_i^u = \sum_{i=1}^{n} dgt_i^u \tag{3}$$

and then send $C_{12\cdots n} \parallel Dgt_i^u$ to the medical personnel.

3.2.4 Data Decryption Phase

After receiving the aggregated data $C_{12\cdots n} \parallel Dgt_i^u$, the medical personnel calculate $r_i^u = H_2\left(r_i^{u-1}\right), i = 1, 2, \cdots, n$, and then verifies:

$$\left(Dgt_i^u - \sum_{i=1}^{n} sk_i\right) modg \stackrel{?}{=} \sum_{i=1}^{n} r_i^u \tag{4}$$

If equal, decrypt $C_{12\cdots n}$ to obtain the aggregated data m:

$$m = \left(\sum_{i=1}^{n} C_{i1} r^{-1} + \cdots + \sum_{i=1}^{n} C_{id} r^{-d} - \sum_{i=1}^{n} r_i^u\right) modg^{'} \tag{5}$$

4 Security Analysis and Proof

In this section, we discuss the security performance of our proposed SEAD scheme. We focus on the attack model in Section 2.3.

Theorem 1. *The proposed scheme can resist eavesdropping/tampering attacks.*

Proof. In our scheme, user data needs to be encrypted and signed before uploading. The attacker can not obtain the user privacy data and tamper with the communication data without knowing the private key SK_i and r of the user and the medical personnel. Therefore, our scheme can resist eavesdropping/tampering attacks. □

Theorem 2. *The proposed scheme can resist user compromise attacks.*

Proof. Our scheme involves two types of secret keys: SK_i and r, SK_i is the shared key between the user u_i and the medical personnel, and r is the shared key of all users and the medical personnel. The attacker compromises one or some network users to obtain the secret key r, it also can not get other user's privacy information. Because the compromised user can not obtain the shared key SK_i of the uncompromised user u_i and the medical personnel. Therefore, our scheme can resist user compromise attacks. □

Theorem 3. *The proposed scheme can resist cloud service compromise attacks.*

Proof. In our scheme, the attacker compromises that the cloud service can not obtain the user's privacy data. Because the cloud service is only responsible for aggregating user data, there is no shared key SK_i between the user and the medical personnel, can not decrypt the user data. Therefore, our scheme can resist cloud service compromise attacks. □

Theorem 4. *The proposed scheme can resist replay attacks.*

Proof. In our scheme, the user will send $C_i \parallel dgt_i^u$ to the base station every time, and the label $dgt_i^u = \left(r_i^u + sk_i\right) modg$ will be updated by updating $r_i^u = H_2\left(r_i^{u-1}\right)$. If the attacker replays the previous interactive message, it will not be able to pass the detection of the medical personnel. Therefore, our scheme can resist replay attacks. □

Theorem 5. *The proposed scheme can provide forward security.*

Proof. In our scheme, the user needs to calculate the mask value $r_i^u = H_2\left(r_i^{u-1}\right)$ before each encryption, and then delete r_i^{u-1}. So even if the attacker compromise the user, can only get the current r_i^u and can not get r_i^{u-1} of the previous time period. Therefore, our scheme can guarantee forward security. □

Table 1: Computational overhead of the three schemes

Scheme	Individual user	Cloud server	Medical personnel
PHDA	$6T_{exp} + 3T_{mul}$	$(2n+3)\,T_p + nT_{exp} + (2n+1)\,T_{mul}$	$2T_p + T_{exp}$
MuDA	$2T_{exp} + T_{mul}$	$(n-1)\,T_{mul}$	$2T_{exp} + 2T_{plm}$
SEDA	$1T_h + 2T_{mad} + dT_{mul}$	$d\,(n-1)\,T_{mad}$	$nT_h + 2T_{mad}$

Table 2: Simulation parameters

Parameters	Values
Size of simulation area/m^2	100×100
Number of mobile nodes	$20, 40, 60, \cdots, 200$
Number of base stations	*1*
Mobile node communication range /m	*50*
Mobile node average velocity /m/s	*1, 2*
Initial energy /mJ	*1000*
MAC layer protocol	*802.11*
Channel bandwidth /Mbs	*11*
Simulation time /s	*100*

5 Performance Evaluation

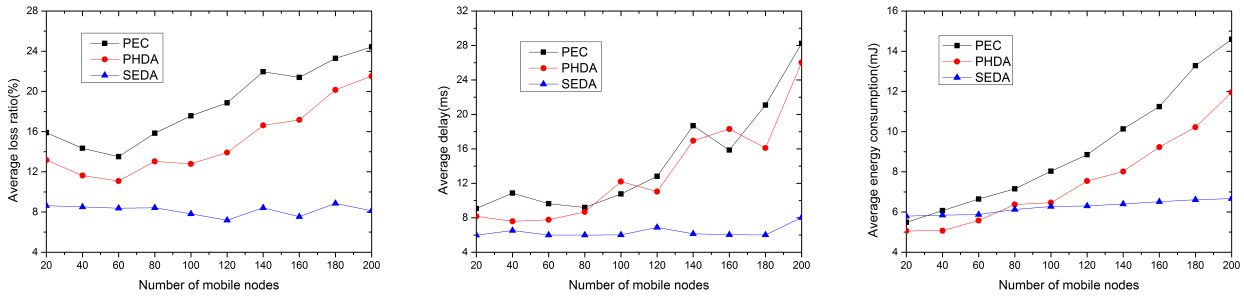
5.1 Computing Complexity

We compare the computational complexity of SEDA with the typical MuDA [1] and PHDA [14] for privacy preserving data aggregation schemes. The computational overhead of each scheme is considered from the following three aspects: the computational cost of a single mobile user, the computational overhead of the cloud service, and the computational overhead of the medical personnel. For SEDA, each mobile user u_i needs to perform 1 hash operation, 2 modulo addition operations and d modular multiplication operations for its privacy data encryption and signature. In the data aggregation phase, the cloud server calculates an encrypted aggregation operation to obtain $C_{12\cdots n}$ need to perform $d(n-1)$ modular addition operation. The medical personnel to verify the signature and decryption data need to n hash operations and 2 modular operations. For PHDA, each mobile user u_i encrypts and signs its health data with 6 exponential modular operations and 3 modular multiplication operations. The cloud service verifies that this received health data signature and aggregation health data requires $(2n+3)$ bilinear pair operations, n exponential exponentiation operations and $(2n+1)$ modular multiplication operations. The medical personnel verify that signature and decryption data requires 2 bilinear pair operations and 1 exponential modular operation. For MuDA, each mobile user u_i encrypts its privacy data requires 2 exponential operations and 1 modular operation. In the data aggregation phase, the cloud server computes an encrypted aggregation operation requires $(n-1)$ modular multiplication operations. The medical personnel decrypts the aggregated health data with 2 bilinear pair operations and 1 discrete logarithmic operation.

The computational complexity of the three schemes is shown in Table 2. Where T_{exp} represents the computational overhead required for exponential modular operation in Z_{N^2}, T_{mul} represents the computational overhead required for modular multiplication operation in $\mathbb{G}$, T_{mad} represents the computational overhead required for modular addition operation in $\mathbb{G}$, T_h represents the computational overhead required for the hash operation, T_p represents the computational overhead required for bilinear pairing operations, T_{plm} represents the computational overhead required to calculate discrete logarithms using Pollard's Lambda method, and n represents the total number of mobile users within the network. As can be seen from Table 1, our scheme is significantly less than the other two schemes, because the bilinear pairing operation and exponential modular operation need to spend much more than the modular operation.

5.2 Simulation Settings

Our simulations are performed in NS-2 [11]. Two main experiments are performed to evaluate the performance of the proposed scheme. In the first experiment, the moving speed of the mobile node was set to 1 m/s. In the second experiment, the moving speed of the mobile node is set to 2 m/s. In all simulation experiment, the mobile nodes are randomly deployed in a $100 \times 100m^2$ monitoring area, the base station node is located in the center of the area. Table 2 shows some basic parameter settings in the simulation. In order to evaluate the transmission efficiency of SEDA health data, there are three different



(a) Loss ratio vs. Number of mobile nodes (b) Delay vs. Number of mobile nodes (c) Energy consumption vs. Number of mobile nodes

Figure 3: The user movement speed is 1m/s

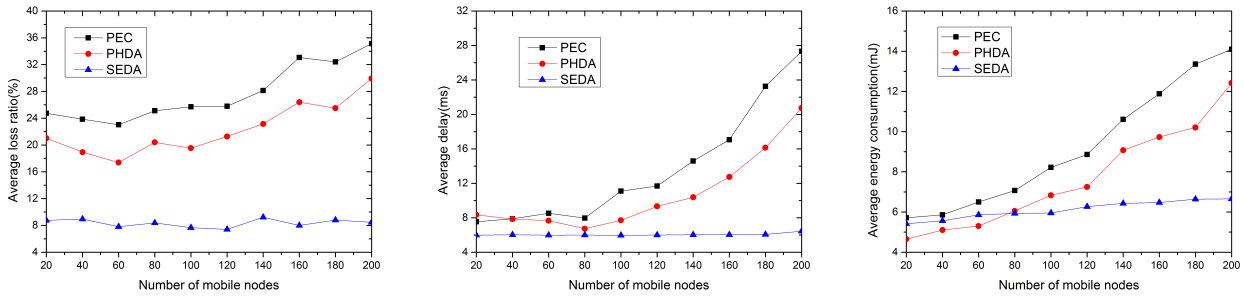
data transmission solutions are considered. The first is PEC [8], a traditional solution of relying on all neighbor nodes to forward the user data. The second is PHDA [14], a method that relies on base stations and any neighbor nodes to forward the user data. The third is our proposed SEDA solution, which relies on the base station and the optimal neighbor nodes to forward the user data.

The performance metrics that we use in simulation experiments are the packet loss ratio, transmission delay and energy consumption. The average packet loss ratio (LR) is defined as $LR = \frac{1}{n-1}\sum_{i=0}^{n-1}\left(M_{AGTs}^{i} - M_{AGTr}^{i}\right)/M_{AGTs}^{i}$, where n represents the number of mobile nodes,M_{AGTs}^{i} represents the total number of the mobile node u_i sends packets of *cbr* (constants bit rate) data flow in the application layer (AGT), and M_{AGTr}^{i} represents the total number of u_i received packets of *cbr* data flow in AGT. The average packet delay (PD) is defined as $PD = \frac{1}{N+1}\sum_{i=0}^{N}\left(T_r^i - T_s^i\right)$, where N represents BS in the AGT layer to receive the total number of packets of *cbr* data flow, T_r^i represents BS receives the $i-th$ packet time, and T_s^i represents u_i sends the $i-th$ packet time. The average energy consumption (EC) is defined as $EC = \frac{1}{n}\sum_{i=0}^{n}\left(E_{init}^{i} - E_{res}^{i}\right)$, where n represents the number of mobile nodes, E_{init}^{i} represents the initial energy value of u_i, and E_{res}^{i} represents the residual energy value of u_i at the end of simulation.

5.3 Simulation Results

In Figure 3, the moving speed of the mobile node is set to 1 m/s. Figure 3(a) shows the relationship between the average packet loss ratio and the number of mobile nodes. As can be seen from the figure, with the increase of the number of mobile nodes, PEC and PHDA packet loss first decreases then increases gradually, because congestion occurs when the area of the coverage area of the mobile node is expanded to a certain extent. SEDA has a low packet loss ratio compared to PEC and PHDA, when the number of mobile nodes is 200, the average loss ratio of SEDA is 66.74% less than PEC and 62.25% less than PHDA. This is because SEDA chooses the best node as the next hop forwarding node, which is not affected by the number of mobile nodes. Figure 3(b) shows the relationship between the average delay and the number of mobile nodes. It can be seen that the average delay of PEC and PHDA is increasing with the number of mobile nodes increasing, while the average delay of SEDA is almost constant. Specifically, when the number of mobile nodes is 200, the average delay of SEDA is 76.4% and 68.93% less than that of PEC and PHDA respectively. This is because the number of forwarding hops for PEC and PHDA is increasing as the number of mobile nodes increases, and SEDA selects the best node as the next hop node, and the hop count does not increase with the number of mobile nodes. Figure 3(c) shows the relationship between the number of mobile nodes and the average energy consumption. As can be seen from the figure, SEDA has a lower energy consumption compared to the other two schemes. Specifically, when the number of mobile nodes is 200, the average energy consumption of SEDA is 54.34% less than PEC and 46.43% less than PHDA. This is because SEDA selects the nearest node to the the target node for forwarding, thereby reducing energy consumption.

In Figure 4, the moving speed of the mobile node is set to 2 m/s. Figure 4(a) shows the relationship between the average loss ratio and the number of mobile nodes. It can be seen from the figure that SCDA has a low packet loss ratio compared to PEC and PHDA, when the number of mobile nodes is 200, the average loss ratio of SEDA is 75.9% less than PEC and 71.71% less than PHDA. As mentioned earlier, this is because SEDA chooses the best node as the next hop node, thereby reducing the number of forwarding hops. Figure 4(b) shows the relationship between the average delay and the number of mobile nodes. This graph shows that SEDA has a low transmission delay compared to the other two schemes. When the number of mobile nodes is 200, the average delay of SEDA is 70.55% and 68.06% less than that of PEC and PHDA. Because SEDA chooses the optimal node as the next hop node, thereby reducing the transmission delay.



(a) Loss ratio vs. Number of mobile nodes (b) Delay vs. Number of mobile nodes (c) Energy consumption vs. Number of mobile nodes

Figure 4: The user movement speed is 2m/s

Table 3: To-be tested audio files

Simulation	Avg. packets loss ratio	Avg. Delay	Avg. Energy consumption
Experiment 1	66.74% and 62.25%	76.4% and 68.93%	54.34% and 46.43%
Experiment 2	75.9% and 71.71%	70.55% and 68.06%	52.8% and 44.25%

Figure 4(c) shows the relationship between the average energy consumption and the number of mobile nodes. It can be seen that SEDA has a lower energy consumption compared to the other two schemes. Specifically, when the number of mobile nodes is 200, the average energy consumption of SEDA is 52.8% and 44.25% less than that of PEC and PHDA, respectively. As mentioned earlier, this is because the energy consumption is also decreasing as the number of forwarding hops decreases.

A comparison between experiment 1 and experiment 2 is shown in Table 3. This table shows how much of the packet loss ratio, delay and energy consumption of SEDA is less than that of PEC and PHDA. When the mobile user's moving speed is 2m/s, experiment 2 has a high packet loss ratio compared to experiment 1. Because as the mobile user's mobile speed becomes faster, the network topology becomes faster, thus affecting the packet delivery ratio. Due to the higher number of packets lost in experiment 2, energy consumption and delay are reduced.

6 Conclusion

In this paper, we propose a secure and efficient data aggregation scheme for cloud-assisted WBAN. The scheme uses privacy homomorphism to encrypt user data so that it does not need to be decrypted when aggregating data, ensuring data confidentiality and resisting compromise attacks. At the same time, the user data is forwarded by using the fixed base station node and the best relay node between the user and the base station, thus improving the transmission efficiency of the user data. The experimental results show that our scheme has lower packet loss ratio, smaller delay and less energy consumption.

Acknowledgments

Above work is supported by National Natural Science Foundation (NSF) of China under grant Nos. 61370007, 61572206, U1405254, Huaqiao University graduate research innovation ability cultivation project of China under grant No. 1511314006, Fujian Provincial Natural Science Foundation of China under grant No. 2013J01241, and Program for New Century Excellent Talents of Fujian Provincial under grant No. 2014FJ-NCET-ZR06.

References

[1] L. Chen, R. X. Lu, Z. F. Cao, K. AlHarbi, and X. D. Lin, "Muda: Multifunctional data aggregation in privacy-preserving smart grid communications," *Peer-to-Peer Networking and Applications*, vol. 8, no. 5, pp. 777–792, 2015.

[2] C. Q. Hu, H. J. Li, Y. Huo, T. Xiang, and X. F. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.

[3] N. Jammali and L. C. Fourati, "Pfka: A physiological feature based key agreement for wireless body area network," in *International Conference on Wireless Networks and Mobile Communications (WINCOM'15*, pp. 1–8, Oct. 2015.

[4] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks," *Procedia Computer Science*, vol. 34, pp. 511–517, 2014.

[5] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A secure and efficient one-time password authentication scheme for WSN," *International Journal Network Security*, vol. 19, no. 2, pp. 177–181, 2017.

[6] C. T. Li, C. C. Lee, and C. Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, p. 117, 2016.

[7] C. T. Li, C. W Lee, and J. J. Shen, "An extended chaotic maps-based keyword search scheme over encrypted data resist outside and inside keyword guessing attacks in cloud storage services," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1601–1611, 2015.

[8] X. H Liang, R. X. Lu, L. Chen, X. D. Lin, and X. M. Shen, "Pec: A privacy-preserving emergency call scheme for mobile healthcare social networks," *Journal of Communications and Networks*, vol. 13, no. 2, pp. 102–112, 2011.

[9] X. D. Lin, R. X. Lu, X. M. Shen, Y. Nemoto, and N Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, 2009.

[10] S. Ozdemir, M. Peng, and Y. Xiao, "Prda: polynomial regression-based privacy-preserving data aggregation for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 15, no. 4, pp. 615–628, 2015.

[11] R. F. S. Pearlin and G. Rekha, "Performance comparison of AODV, DSDV and DSR protocols in mobile networks using NS-2," *Indian Journal of Science and Technology*, vol. 9, no. 8, pp. 130–141, 2016.

[12] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in wireless body area network (wban)," in *15th International Conference on Advanced Communication Technology (ICACT'13)*, pp. 998–1001, Jan. 2013.

[13] Q. Wang, C. Wang, K. Ren, W. J. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[14] K. Zhang, X. H. Liang, M. Baura, R. X. Lu, and X. M. Shen, "Phda: A priority based health data aggregation with privacy preservation for cloud assisted wbans," *Information Sciences*, vol. 284, pp. 130–141, 2014.

[15] J. Zhou, Z. F. Cao, X. L. Dong, and X. D. Lin, "Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions," *IEEE Wireless Communications*, vol. 22, no. 2, pp. 136–144, 2015.

[16] J. Zhou, Z. F. Cao, X. L. Dong, N. X. Xiong, and A. V. Vasilakos, "4s: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Information Sciences*, vol. 314, pp. 255–276, 2015.

Biography

Huaijin Liu received the B.S. degree from Huaqiao University, China, in 2015, where he is currently pursuing the master's degree. His current research interest includes wireless sensor network security, wireless body area network security and privacy protection, wireless vehicle network security.

Yonghong Chen received the B.S. degrees from Hubei National University, and M.Eng. and Ph.D. degree degrees from Chognqing University, Chongqing, China, in 2000 and 2005 respectively. He is currently the professor of of College of Computer Science and Technology, Huaqiao University, Xiamen, China. His research interests include network security, watermarking and nonlinear processing.

Hui Tian received his BSc and MSc degrees in Wuhan Institute of Technology,Wuhan, China in 2004 and 2007, respectively. He received his PhD degree in Huazhong University of Science and Technology, Wuhan, China. He is now an associate professor in the National Huaqiao University of China. His research interests include network and multimedia information security, digital forensics and information hiding.

Tian Wang received his BSc and MSc degrees in Computer Science from the Central South University in 2004 and 2007, respectively. He received his PhD degree in City University of Hong Kong in 2011. Currently, he is a professor in the Huaqiao University of China. His research interests include wireless sensor networks, fog computing and mobile computing.

Yiqiao Cai received the B.S. degree from Hunan University, Changsha, China, in 2007, and the Ph.D. degree from Sun Yat-sen University, Guangzhou, China, in 2012. In 2012, he joined Huaqiao University, Xiamen, China, where he is currently a lecturer with the College of Computer Science and Technology. He is interested in differential evolution, multiobjective optimization, and other evolutionary computation techniques.