Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 4028196, 7 pages
https://doi.org/10.1155/2018/4028196

Research Article

Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks

Chen Wang[1,2] **Wenying Zheng**[3] **Sai Ji**[4] **Qi Liu**[4] **and Anxi Wang**[4]

[1] *The School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[2] *Guangxi Key Laboratory of Cryptography and Information Security, Guilin, China*
[3] *The School of Applied Meteorology, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[4] *The Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing 210044, China*

Correspondence should be addressed to Wenying Zheng; zhengwy0501@126.com

Received 11 April 2018; Revised 31 May 2018; Accepted 20 June 2018; Published 5 August 2018

Academic Editor: Ding Wang

Smart mobile devices are one of the core components of the wireless body area networks (WBANs). These devices shoulder the important task of collecting, integrating, and transmitting medical data. When a personal computer collects information from these devices, it needs to authenticate the identity of them. Some effective schemes have been put forward to the device authentication in WBANs. However, few researchers have studied the WBANs device authentication in emergency situations. In this paper, we present a novel system named emergency medical system without the assistance of doctors. Based on the system, we propose an identity-based fast authentication scheme for smart mobile devices in WBANs. The scheme can shorten the time of device authentication in an emergency to achieve fast authentication. The analysis of this paper proves the security and efficiency of the proposed scheme.

1. Introduction

Nowadays, people's quality of life is improving with the development of society and technology [1]. People's pursuit of happy life has a broader definition. With the continuous improvement of medical level, the phenomenon of aging has appeared in many developed and developing countries. People are in urgent need of a more complete medical system to ensure health and safety. Real time health monitoring is needed to prevent the possibility of chronic diseases and also for emergency treatment of sudden diseases.

Wireless body area network (WBAN) is a network composed of sensor nodes, personal terminals, and medical cloud platforms [2–6]. WBANs can be used to monitor user signs, feed back on real-time data, provide corresponding treatment plan, and make relevant emergency measures. WBANs can not only monitor medical information and vital signs such as body temperature, pulse, and blood pressure through the attachment of sensor nodes, but also inject drugs with the help of embedded actuators to achieve long-term treatment, remote treatment, and emergency treatment. Some researchers consider that WBANs consist of three parties, including patients, doctors, and cloud servers [7–10]. In fact, in some emergency cases, the participation of doctors may not be able to participate in the treatment timely. These emergency cases include falls, myocardial infarction, and stroke. If all the treatments have to wait for the doctor to confirm, the best treatment period might be missed. In this paper, we think that WBAN is mainly composed of three parts: smart mobile devices (SMDs), personal digital assistants (PDAs), and remote cloud servers (RCSs) [11, 12]. An SMD is a portable sensor or actuator that has certain computing power and can perceive the specific information of the outside world. SMDs are indispensable parts of WBANs. SMDs can be utilized not only as a channel for WBANs to perceive external information, but also as a means for WBANs to intervene in the outside world. PDA can be a kind of mobile computing terminal with personal computers, smart phones, and so on. PDA is responsible for receiving messages collected by SMD or issuing commands to SMD. The RCS is responsible for storing and analyzing medical data and feedback treatment recommendations [13, 14].

Motivation of This Paper. Most of the existing schemes for WBAN do not consider how to implement emergency treatment without doctors' participation, so as to alleviate the sudden exacerbation of the patient's disease. The existing authentication scheme cannot be efficient and fast for such situations.

Our Contributions. The contributions of this paper can be concluded as the following three points. We first discuss a special case of how to perform treatment when a patient meets a sudden illness. The case is taken as the environment of the proposed system and scheme. We then propose an emergency medical system without the assistance of medical staff. Based on the system, we present the novel scheme to achieve fast authentication for smart mobile devices in WBANs. The detailed contributions are listed as follows.

(i) **A special case is discussed.** When the monitored object is suffering from sudden onset of myocardial infarction and stroke, WBANs are needed for emergency treatment. Under such circumstances, the traditional three-party system of patients, doctors, and medical cloud is no longer applicable. This paper discusses the particularity of this case and further studies on it.

(ii) **An emergency medical system has been proposed.** Based on the discussed case, we provide a system design that can be applied to this case. The novel emergency medical system is mainly composed of smart mobile devices, personal digital assistants, and remote cloud servers.

(iii) **An identity-based fast authentication scheme is proposed.** Finally, we propose an identity-based fast authentication scheme for smart mobile devices in WBANs. The scheme can quickly realize the identity authentication of a device and provide a reliable precondition for further encrypted data transmission of the system.

Organizations. The remainder of this paper is organized as follows. Section 2 presents some related works. Section 3 illustrates some preliminaries of this paper, including bilinear pairing, system model, and system components. Section 4 shows the security models of the novel authentication scheme. Section 5 presents the proposed scheme in detail. Section 6 states the security analysis of the proposed scheme. Section 7 presents the performance analysis of the scheme with simulations on PBC. Finally, the conclusions are drawn in Section 8.

2. Related Works

Many researchers have studied the authentication of smart mobile devices in WBANs.

Wang et al. [15] present an overview of attacks, principle, and solutions on the anonymity of two-factor authentication schemes. To improve the current schemes from being stuck with the security-usability tension, the scheme proposed by Wang et al. [16] can resolve the various issues arising from user corruption and server compromise.

Chiou et al. [17] propose a scheme which guarantees anonymity, unlinkability, and message authentication for uses. The proposed scheme also allows patients to directly and remotely consult with doctors in a safe way.

Li et al. [18] present participant authentication in mobile emergency medical care systems for patients supervision. They propose a secure cloud-assisted architecture for accessing and monitoring health in WBANs. Chaotic maps based authentication and key agreement mechanisms are utilized to provide data security and mutual authentication. Based on the proposed scheme, Li et al. [19] design another dynamic identity and chaotic maps based authentication scheme and a secure data protection approach to prevent illegal intrusions for medical systems. They also propose an improved secure authentication and data encryption scheme for the smart devices in medical systems in [20].

Li et al. [21] propose an anonymous mutual authentication for centralized two-hop WBAN. The scheme allows sensor nodes attached to the patient's body to authenticate with the local server/hub node.

Das et al. [22] find that some existing schemes are still vulnerable to privileged-insider attack. So they present a smartcard-based anonymous user authentication scheme for medical systems to be secure against possible known attacks.

To achieve secure and authorized communication, a symmetric key based authentication protocol is designed for medical system by Srinivas et al. [23]. They claimed that the results show that their scheme reaches the level of security requirements and has suitable cost for applications in medical environment.

Some researchers achieve security authentication in WBANs with some novel technologies. For instance, Hayajneh et al. [24] propose a scheme based on the Rabin authentication algorithm. They modify the algorithm to improve its signature signing process for delay-sensitive applications in WBANs. Park et al. [25] propose a selective group authentication scheme using Shamir's threshold technique. They prove that their scheme can achieve efficient user authentication and conditional access authority for devices in medical systems.

Mohit et al. [26] achieve mutual authentication between healthcare center, cloud server, and patients, which can support patient anonymity and resist strong security attacks such as nonrepudiation and confidentiality of data.

Li et al. propose a scheme to resist Denial of Service (DoS) attack [27]. To further solve problems in WBANs, Li et al. [28] provide three protocols for different tiers. The three protocols allow the anonymous authentication among mobile users, controller nodes, and the medical server.

3. Preliminaries

Here are some preliminaries provided for the proposed scheme.

3.1. Bilinear Pairing. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two groups of prime order q. Let $\mathbb{G}_1$ be an additive group and $\mathbb{G}_2$ be a multiplicative group. e is set to be as a mapping on $(\mathbb{G}_1, \mathbb{G}_2) : \mathbb{G}_1^2 \longrightarrow \mathbb{G}_2$. The cryptographic bilinear map e satisfies the following properties.

Bilinearity. $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in Z_q^*$. This can be expressed in the following manner. For $P, Q, R \in \mathbb{G}_1$, $e(P + Q, R) = e(P, R)e(Q, R)$.

Nondegeneracy. If P is a generator of $\mathbb{G}_1$, then $e(P, P)$ is a generator of $\mathbb{G}_2$. In other words, $e(P, P) \neq 1$.

Computability. e is efficiently computable.

3.2. System Model. In this subsection, we provide the introduction of the novel system in this paper. The system is named as emergency medical system. Figure 1 shows a schematic diagram of the system. The system is composed of sensors, actuators, PDA, and the cloud. Sensor nodes are responsible for collecting medical information in the WBAN. All data from the sensor nodes are compiled by PDA. The cloud will receive a summary of the information that PDA sends to it. According to cloud analysis of the current data and comparison of historical data, a treatment plan is chosen. The treatment plan will be directly sent to various actuators in a concise way, and the whole treatment plan will be sent to PDA.

3.3. System Components. The components of the system include smart mobile devices (SMDs), personal digital assistants (PDAs), and remote cloud servers (RCSs). The three main components are introduced as follows.

Smart Mobile Devices (SMDs). SMDs are sensors or actuators with certain computing ability in WBANs. Sensors are responsible for perceiving vital signs of patients. The important user medical data collected is transmitted by sensors in some specific form. The actuators are responsible for specific treatment operations after receiving instructions, such as injection of adrenaline and electric shock.

Personal Digital Assistants (PDAs). PDAs are personal computers or smart phone taken by the patient. As a link between smart devices and cloud servers, PDA is responsible for transmitting SMD's collected information and RCS's instructions.

Remote Cloud Servers (RCSs). The RCS is often a group of distributed computers with super computing power and large storage space. For ease of interpretation, we usually think that RCS's computing power and storage space are infinite.

4. Security Model

In this section, the security model of this paper is provided. Note that the key generation center (KGC) utilized in this paper is considered as a trusted third party to generate some system parameters [29–32].

4.1. A Forged SMD. We assume that a forged SMD may try to send the wrong message with the legal identity of the original SMD. Once such behavior is successful, it will be very dangerous for patients in the medical system. For example, a patient has no stroke, and the node passes the authentication and sends a stroke message to PDA, which could lead to the final error diagnosis of the patient and the treatment of the patient with the wrong medicine.

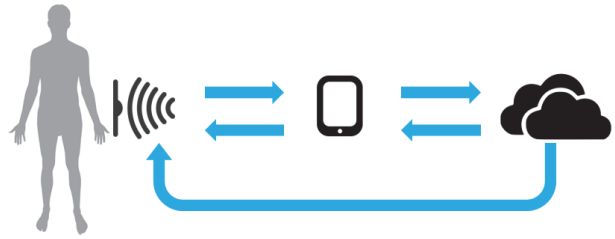

Figure 1: A schematic diagram of the emergency medical system.

4.2. Men-in-the-Middle Attack. Men-in-the-Middle (MITM) attack refers to the attack that the attacker intercepts the message and attempted to tamper with the medical message. This kind of attack will cause the original information to be destroyed, which leads the system to be unable to pass the authentication of SMD. We assume that an MITM attacker have the ability to block the message and implement all necessary calculations.

4.3. Replay Attack. Replay attack means that the attacker collects authentication messages sent before SMD and sends to PDA, trying to pass the authentication by PDA. This attack uses a message that has been authenticated. If the scheme is not well designed, the old authentication message is likely to be used by malicious users to achieve their goals. We assume that the attacker have the ability to obtain the historical authentication message and resubmit it.

5. Our Proposed Authentication Scheme

The proposed scheme is introduced detailedly in this section.

5.1. Overview of the Scheme. The whole scheme consists of three main phases: device fast authentication, secure message transmission, and secure instruction distribution. The whole scheme is shown in Figure 2. The circles in Figure 2 represent SMDs, including sensors and actuators, and the rectangle represents a PDA. A certain amount of SMDs are deployed on the patient. When a sudden illness occurs, one or more SMDs will monitor the change of corresponding parameters and integrate medical data information. Subsequently, SMDs need to prove identities and transmit encrypted information to the PDA. Then, the PDA needs to transmit the message to the RCS. These steps are the device fast authentication and secure message transmission that we mentioned earlier. RCS analyzes the current data with its powerful computing power and compares the data with the stored historical data. After a corresponding treatment decision is formulated, the RCS reaches the treatment instruction by secure instruction distribution phase. In this paper, we focus on the method of device fast authentication. We will provide some feasible solutions of the other phases for reference.

5.2. Device Fast Authentication. This authentication method is the main innovation of our paper. The detailed exposition will be carried out in this subsection. The device fast authentication consists of three algorithms: registration,

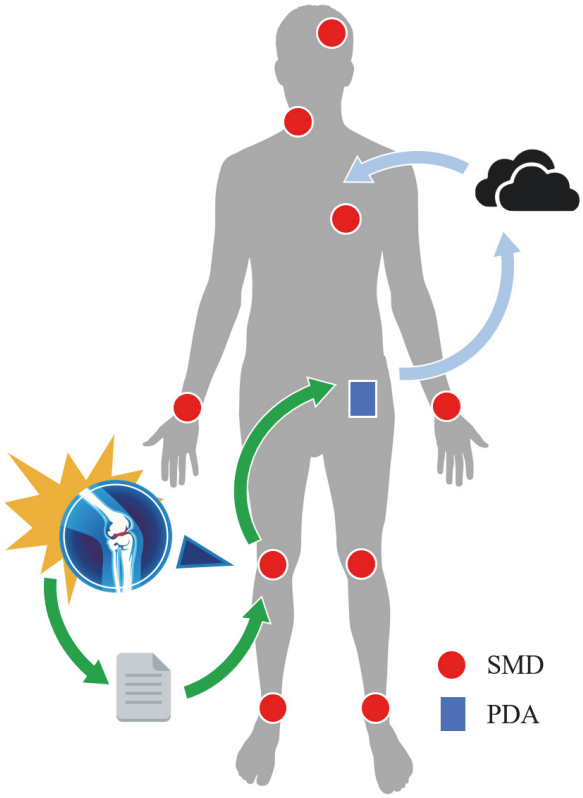

Figure 2: Illustration of the proposed scheme.

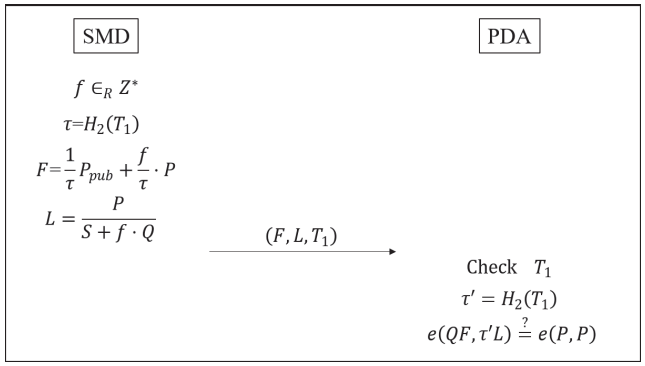

Figure 3: The process of device fast authentication.

authentication information delivery, and identity authentication. We will provide the detailed description of the three algorithms. The authentication information delivery and identity authentication are illustrated in Figure 3.

Registration. When every SMD enters WBAN, it needs to register with KGC.

KGC chooses a random number λ. Let a point P on $\mathbb{G}_1$ be a generator. The system public key is computed as $P_{pub} = \lambda \cdot P$. Choose two hash functions H_1 and H_2 as $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1^*$ and $H_1 : \{0,1\}^* \longrightarrow \{0,1\}^l$, where l represents a length of the number. Suppose that the identity of a SMD is ID. The public key of the SMD is $Q = H_1(ID)$ and secret key $S = \lambda \cdot Q$. The system parameter will be written into the memory of the SMD.

Authentication Information Delivery. If the SMD wants to transmit message, its identity needs to be authenticated.

SMD first chooses a random number f. A current timestamp T_1 is recorded and hashed as $\tau = H_2(T_1)$. Authentication information F and L will then be calculated as follows.

$$F = \frac{1}{\tau} P_{pub} + \frac{f}{\tau} \cdot P,$$
$$L = \frac{P}{S + f \cdot Q}, \tag{1}$$

where τ is the hashed timestamp, P_{pub} is the public key of the system, f is the random number chosen by SMD, P represents the generator of the system, Q refers to the hashed ID, and S is the secret key of SMD.

The authentication information file is organized as (F, L, T_1), which is then sent to PDA for authentication.

Identity Authentication. After the authentication information file is received, PDA first checks T_1 to figure out whether the message is delayed when being transmitted. Then, $\tau' = H_2(T_1)$ is performed to calculate the hash value of the timestamp. Finally, PDA determines whether the device is a trusted one by the following formula.

$$e\left(QF, \tau' L\right) \stackrel{?}{=} e\left(P, P\right), \tag{2}$$

where Q is the hashed identity of the SMD, τ' is the hashed timestamp calculated by the PDA itself, and $e(P, P)$ can be computed offline.

5.3. Secure Message Transmission and Secure Instruction Distribution. The two algorithms, which are named as secure message transmission and secure instruction distribution, are both encryption methods. The encryption methods are proven to be safe in WBAN and can be utilized in our system.

We consider two entities in these algorithms: sender and receiver. The registration phase of the sender is the same as what is introduced in the algorithm of device fast authentication. The hashed identities of the sender and receiver are Q_1 and Q_2. The secret keys of the sender and the receiver are S_1 and S_2.

The sender first chooses random number r and computes $R = r \cdot P$. Then, the sender calculates $y = e(1/P, 1/Q_1 P)^r$.

Then the sender computes encrypted message file M with plaintext m:

$$M = m \oplus H_3\left(y\right), \tag{3}$$

where H_3 is a hash function: $H_3 : \{0,1\}^* \longrightarrow \{0,1\}^h$ and h is the length of the message file m.

The final parameter E is calculated as

$$E = \frac{S_1}{Q_2 S_1 R} + \frac{r}{Q_2 S_1 R}. \tag{4}$$

The file (M, E, R) will be sent to the receiver.

The receiver calculates parameter B as

$$B = \frac{S_2}{Q_1 P_{pub} + R}. \tag{5}$$

Let $y' = e(B, E)$ and $m = M \oplus H_3(y')$.

According to the above steps, the collected medical data or the instruction data can be transmitted to the receiver safely and acquired.

6. Security Analysis

In this section, the correctness and security against a forged SMD, MITM attack, and replay attack of our proposal are proved.

6.1. Correctness. The correctness of device fast authentication is proved as follows:

$$\begin{aligned} & e\left(QF, \tau' L\right) \\ &= e\left(Q\left(\frac{1}{\tau} P_{pub} + \frac{f}{\tau} \cdot P\right), \tau'\left(\frac{P}{S + f \cdot Q}\right)\right) \\ &= e\left(\frac{PQ}{\tau}(\lambda + f), \tau' P \frac{1}{\lambda Q + fQ}\right) \\ &= e\left(\frac{Q}{\tau}(\lambda + f) P, \frac{\tau'}{Q} \frac{1}{\lambda + f} P\right) \overset{if \tau = \tau'}{=} e(P, P) \end{aligned} \tag{6}$$

Obviously, if $\tau = \tau'$, $e(QF, \tau' L) = e(P, P)$. In fact, τ and τ' are computed with the same timestamp and hash function, so the authentication process is correct and efficient.

The correctness of the message transmission scheme for secure message transmission and secure instruction distribution is proved as follows:

$$\begin{aligned} y' &= e(B, E) = e\left(\frac{S_2}{Q_1 P_{pub} + R}, \frac{S_1}{Q_2 S_1 R} + \frac{r}{Q_2 S_1 R}\right) \\ &= e\left(\frac{\lambda Q_2}{(Q_1 \lambda + r) P}, \frac{\lambda Q_1 + r}{Q_2 \lambda Q_1 r P}\right) = e\left(\frac{1}{P}, \frac{1}{Q_1 P}\right)^r \\ &= y \end{aligned} \tag{7}$$

It can be seen from the proof that the values of y and y' are equal; obviously the recalculated m by y' is the same as the real one. So the design of the transmission scheme is also correct.

6.2. Security against a Forged SMD. A forged SMD may falsify the authentication information in order to pass the authentication. He can get the current timestamp to calculate τ. He can also select a random number f to calculate $F = (1/\tau) P_{pub} + f/\tau \cdot P$. Actually, the forged SMD has no opportunity to obtain the value of S. So he cannot calculate $L = P/(S + f \cdot Q)$. To sum up, our scheme can resist the attack by a forged SMD.

Table 1: Computational cost comparison.

Phases	SMD	PDA
Authentication information delivery	1H+3M	/
Identity authentication	/	1H+1M+1P

6.3. Security against Men-in-the-Middle Attack. MITM attack may cause medical information to be replaced or tampered in the middle. An adversary may calculate a fake secret key $S' = \lambda' Q$ and choose a new random number f' and replace the value τ with a new hashed timestamp T_2, remarked as τ_2. In fact, he still cannot pass the authentication. The new F' and L' can be calculated as follows:

$$\begin{aligned} F' &= \frac{1}{\tau_2} P_{pub} + \frac{f'}{\tau_2} \cdot P, \\ L' &= \frac{P}{S' + f' \cdot Q}. \end{aligned} \tag{8}$$

The faked file (F', L', T_2) will be sent to the PDA. PDA computes $\tau_2 = H_2(T_2)$. $e(QF, \tau_2 L)$ is computed as follows:

$$\begin{aligned} & e\left(QF, \tau_2 L\right) \\ &= e\left(Q\left(\frac{1}{\tau_2} P_{pub} + \frac{f'}{\tau_2} \cdot P\right), \tau_2\left(\frac{P}{S' + f' \cdot Q}\right)\right) \\ &= e\left(\frac{PQ}{\tau_2}\left(\lambda + f'\right), \tau_2 P \frac{1}{\lambda' Q + f' Q}\right) \\ &= e\left(\frac{Q}{\tau_2}\left(\lambda + f'\right) P, \frac{\tau_2}{Q} \frac{1}{\lambda' + f'} P\right) \\ &= e\left(\left(\lambda + f'\right) P, \frac{1}{\lambda' + f'} P\right) \neq e(P, P) \end{aligned} \tag{9}$$

It is not difficult to see that the new parameters of the MITM can not be certified.

6.4. Security against Replay Attack. An attacker who implements replay attack can try to pass the authentication by collecting files previously sent by SMD and sending an old file to PDA. In fact, there is a timestamp in the file. If the time difference between the timestamp and the time in which the file is accepted by PDA is beyond the range of the delay tolerance, the file will be identified as an invalid one. If the attacker tampered with the timestamp, he could not calculate the F matched with the new timestamp because the random number f is unknown.

7. Performance Analysis

The performance of the proposed scheme is discussed in this section. The computational cost of different entities in the proposed scheme is shown in Table 1. We take into consideration the computational costs of SMD and PDA. We consider the cost of collision-resistant hash function, bilinear pairing, and scalar multiplication [33]. In Table 1, M represents scalar multiplication, P denotes bilinear pairing,

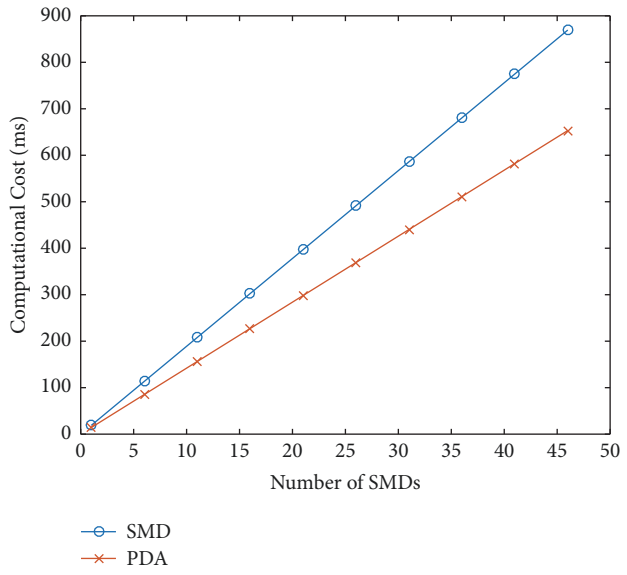

Figure 4: The time cost of SMD and PDA in the emergency medical system.

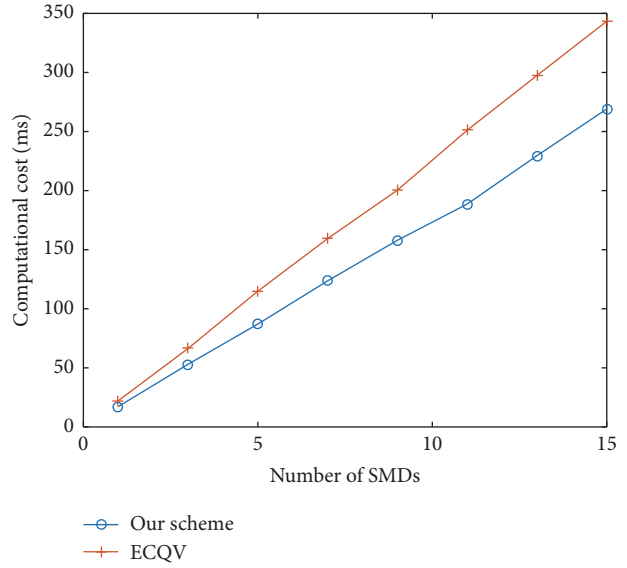

Figure 5: The time cost of an SMD in our scheme and ECQV.

and H represents collision-resistant hash function operation. The result comes out that the SMD costs 1 scalar multiplication and 1 collision-resistant hash function operation for sending the authentication message to the PDA. The PDA costs 1 scalar multiplication, 1 bilinear pairing, and 1 collision-resistant hash function operation to certificate the identity of SMD.

The efficiency of the proposed scheme is simulated on GNU Multiple Precision Arithmetic (GMP) library and Pairing-Based Cryptography (PBC) library (https://crypto.stanford.edu/pbc/). C language is utilized on a Linux system with Ubuntu 16.04 TLS, a 2.60 GHz Intel(R) Xeon(R) CPU E5-2650 v2, and 8 GB of RAM. The results are shown in Figure 4. Because SMDs and PDA are resources limited devices, controlling their computing resources consumption is very important. Our simulation reflects the time summation of all SMDs and the time cost of PDA when multiple SMDs send authentication requests to PDA. Because the number of devices in WBAN is limited, the simulation results show that our design can effectively reduce the computational cost of PDA. Figure 5 shows the comparison between the novel protocol and ECQV [34]. We can see that when the number of SMDs increase, the computational cost of our novel scheme is lower.

8. Conclusion

In this paper, we discuss the emergency situations in WBANs where the participation of doctors will seriously reduce the efficiency of treatment. In order to solve the problem of emergency treatment, we propose an emergency medical system. Based on the system, an identity-based fast authentication scheme for smart mobile devices in WBANs is proposed. In addition, we also provide a message transmission scheme to improve the system. The authentication scheme is proven to be secure and efficient in our analysis and simulation.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant no. 61672295, no. 61672290, no. U1405254, and no. 61772280, Guangxi Key Laboratory of Cryptography and Information Security under Grant no. GCIS201715, the State Key Laboratory of Information Security under Grant no. 2017-MS-10, the 2015 Project of six personnel in Jiangsu Province under Grant no. R2015L06, the CICAEET fund, and the PAPD fund.

References

[1] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 76, pp. 37–48, 2016.

[2] X. F. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386–2396, 2014.

[3] J. Shen, A. Wang, C. Wang, J. Li, and Y. Zhang, "Content-centric group user authentication for secure social networks," *IEEE Transactions on Emerging Topics in Computing*, 2017.

[4] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2363–2373, 2016.

[5] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE*

Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 912–925, 2018.

[6] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[7] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, pp. 1-1, 2017.

[8] J. Wang, X. Chen, J. Li, J. Zhao, and J. Shen, "Towards achieving flexible and verifiable search for outsourced database in cloud computing," *Future Generation Computer Systems*, vol. 67, pp. 266–275, 2017.

[9] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[10] J. Shen, C. Wang, and A. Wang, "Intelligent agent-based region division scheme for mobile sensor networks," *Soft Computing*, 2018.

[11] C.-F. Lai, S. Zeadally, J. Shen, and Y.-X. Lai, "A cloud-integrated appliance recognition approach over internet of things," *Journal of Internet Technology*, vol. 16, no. 7, pp. 1157–1168, 2015.

[12] J. Shen, C. Wang, A. Wang, Q. Liu, and Y. Xiang, "Moving centroid based routing protocol for incompletely predictable cyber devices in Cyber-Physical-Social Distributed Systems," *Future Generation Computer Systems*, 2017.

[13] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 546–556, 2015.

[14] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive and Mobile Computing*, vol. 41, pp. 219–230, 2017.

[15] D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," *Computer Networks*, vol. 73, pp. 41–57, 2014.

[16] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, pp. 1-1, 201.

[17] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, vol. 40, no. 4, article 101, 15 pages, 2016.

[18] 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, article 117, 15 pages, 2016.

[19] C.-T. Li, C.-C. Lee, C.-Y. Weng, and S.-J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *Journal of Medical Systems*, vol. 40, no. 11, article 233, 10 pages, 2016.

[20] C. Li, T. Wu, C. Chen, C. Lee, and C. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, 1482, 18 pages, 2017.

[21] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, no. 2, pp. 429–443, 2017.

[22] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1899–1933, 2017.

[23] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *Journal of Medical Systems*, vol. 41, no. 5, article 80, 19 pages, 2017.

[24] T. Hayajneh, B. J. Mohd, M. Imran, G. Almashaqbeh, and A. V. Vasilakos, "Secure authentication for remote patient monitoring withwireless medical sensor networks," *Sensors*, vol. 16, no. 4, article 424, 25 pages, 2016.

[25] Y. Park and Y. Park, "A selective group authentication scheme for IoT-based medical information system," *Journal of Medical Systems*, vol. 41, no. 4, article 48, 8 pages, 2017.

[26] P. Mohit, R. Amin, A. Karati, G. P. Biswas, and M. K. Khan, "A standard mutual authentication protocol for cloud computing based health care system," *Journal of Medical Systems*, vol. 41, no. 4, article 50, 13 pages, 2017.

[27] X. Li, J. Niu, M. Karuppiah, S. Kumari, and F. Wu, "Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications," *Journal of Medical Systems*, vol. 40, no. 12, article 268, 12 pages, 2016.

[28] X. Li, M. H. Ibrahim, S. Kumari, and R. Kumar, "Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors," *Telecommunication Systems*, vol. 67, no. 3, pp. 1–26, 2017.

[29] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 4, pp. 567–580, 2009.

[30] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Systems Journal*, vol. 12, no. 1, pp. 916–925, 2018.

[31] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[32] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Networks*, vol. 20, no. 2, pp. 1–15, 2014.

[33] X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, and K. Kim, "Identity-based chameleon hashing and signatures without key exposure," *Information Sciences*, vol. 265, pp. 198–210, 2014.

[34] J. Shen, S. Chang, Q. Liu, and Y. Ren, "Implicit authentication protocol and self-healing key management for WBANs," *Multimedia Tools & Applications*, vol. 77, no. 9, pp. 11381–11401, 2018.