A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications

Mengxia Shuai, University of Science and Technology of China, Anhui, China
Nenghai Yu, University of Science and Technology of China, Anhui, China
Hongxia Wang, Southwest Jiaotong University, Chengdu, China
Ling Xiong, Xihua University, Chengdu, China
Yue Li, Southwest Jiaotong University, Chengdu, China

ABSTRACT

Security and privacy issues in wireless medical sensor networks (WMSNs) have attracted lots of attention in both academia and industry due to the sensitiveness of medical system. In the past decade, extensive research has been carried out on these security issues, but no single study exists that addresses them adequately, especially for some important security properties, such as user anonymity and forward secrecy. As a step towards this direction, in this paper, the authors propose a lightweight three-factor anonymous authentication scheme with forward secrecy for personalized healthcare applications using only the lightweight cryptographic primitives. The proposed scheme adopts pseudonym identity technique to protect users’ real identities and employs one-way hash chain technique to ensure forward secrecy. Analysis and comparison results demonstrate that the proposed scheme can not only reduce execution time by 34% as compared with the most effective related schemes, but also achieve more security and functional features.

KEYWORDS

Authentication, Forward Secrecy, Privacy Protection, User Anonymity, Wireless Medical Sensor Networks

INTRODUCTION

The Internet of Things (IoT) is an emerging mode of modern wireless telecommunications, which allows objects to be sensed or controlled remotely over existing network infrastructure. By combining with cloud computing and fog computing (Qi, Zhang, Dou, & Ni, 2017; Gill, Chana, & Buyya, 2017; Qi, Yu, & Zhou, 2017; Gong, Qi, & Xu, 2018; Qi et al., 2018a), IoT devices can be used to build many service-based applications, such as smart devices (Cui, Zhang, Cai, Liu, & Li, 2018; Cheng, Xu, Tang, Sheng, & Cai, 2018), smart home (Liu, et al., 2018) and security-related applications (Wang, Li, Shi,
Lian, & Ye, 2016; Qi, Zhou, Yu, & Liu, 2017; Ma, Luo, Li, Bao, & Zhang, 2018; Zhang, Qin, Zhang, Liu, & Luo, 2018; Qi et al., 2018b). IoT devices can also be used to enable remote health monitoring, which is a new field known as wireless medical sensor networks (WMSNs). WMSNs have attracted lots of attention in both academia and industry because of the potential in improving the quality of medical services (Walczak & Mann, 2010; Lee, Ghapanchi, Talaei-Khoei, & Ray, 2015). Through WMSNs, healthcare professionals are able to access the patients’ sensitive data collected from the medical sensor nodes which are placed on/in patients’ bodies, and provide remote medical treatment, emergency medical assistance or give some constructive advice on the patients’ further treatment.

A typical structure of WMSNs for personalized healthcare applications is demonstrated in Figure 1. Although WMSNs bring a lot of convenience to people’s life (Siddesh et al., 2017), security and privacy issues in WMSNs are becoming great challenges due to the sensitiveness of medical system (Ameen, Liu, & Kwak, 2012; Xu, Qi, Dou, & Yu, 2017). The medical data collected from the medical sensor nodes is sensitive, and the privacy of these data is protected legally. Due to the open feature of wireless communication, an adversary can intercept and alter the transmitted messages easily. Once obtaining these sensitive data, an adversary may acquaint the disease what the patient has and profit financially by selling sensitive data, it is a serious violation of the patient’s privacy. Further, the adversary can even misreport or distort the patient’s physiological data to cause physical harm, it may result in improper diagnosis and treatment. Therefore, it is very important to design an effective authentication scheme to guarantee secure communication and protect patients’ privacy in WMSNs.

Related Work

In the past decade, many authentication schemes are proposed to solve the security issues in WMSNs. In 2007, Hu et al. (2007) designed a telecardiology sensor network platform for real-time healthcare data collection using the symmetric cryptography. Two years later, Huang et al. (2009) presented

Figure 1. A typical structure of WMSNs
a healthcare monitoring architecture for monitoring elderly or chronic patients in their residence, which used Advanced Encryption Standard (AES) algorithm to provide authentication and secret communication. Unfortunately, neither of them could achieve mutual authentication successfully. In 2009, Malasri et al. (2009) designed a secure WMSN system for healthcare based on symmetric cryptography and elliptic curve cryptography (ECC), they implemented their mechanisms on a wireless mote platform. Later, Das (2009) presented a two-factor user authentication protocol for WSN and claimed their protocol could provide strong authentication and resist various attacks. Unfortunately, Khan et al. (2010) pointed out that Das’s scheme (Das, 2009) was vulnerable to privileged-insider attack and Gateway node (GWN) bypass attack. In 2012, Kumar et al. (2012) presented an efficient and strong authentication protocol, named E-SAP, for healthcare application using WMSNs. They demonstrated that their protocol was more secure against many practical attacks. But later, He et al. (2015) in 2015 pointed out that the scheme proposed by Kumar et al. failed to resist some known attacks, liking off-line password guessing attack and privileged insider attack. To overcome their security shortcomings, they proposed a robust anonymous authentication protocol for healthcare applications using WMSNs. One year later, Li et al. (2016) pointed out that He et al.’s scheme (He et al., 2015) was not only incorrect in authentication and session key agreement phase, but also lacked wrong password detection mechanism. Further, they proposed a new user anonymous authentication protocol based on WMSNs. In their scheme, the biometric was introduced as the third authentication factor. Similarly, Mir et al. (2017) also showed that He et al.’s scheme (He et al., 2015) still suffered from various security flaws, including inefficient login phase, password guessing attack, forward secrecy. They also proposed an improved scheme and claimed that their scheme was secure in forward secrecy. However, the authors find out their scheme is still prone to forward secrecy attack. An adversary can guess the user identity offline through the transmitted message if GWN’s secret key is compromised, the adversary can further compute the session key. Hence, Mir et al.’s scheme (Mir et al., 2017) failed to achieve forward secrecy. At the same year, Wu et al. (2017) also claimed that He et al.’s scheme (He et al., 2015) still had some vulnerabilities, including off-line password guessing attack, the impersonation attack and the sensor node capturing attack. Hence, they proposed an energy-efficient scheme with a lightweight design for WMSNs. But later, Srinivas et al. (2017) observed that Wu et al.’s scheme was not only failed to resist various attacks, such as off-line guessing attack, privileged insider attack and new smart card issue attack, but also not suitable for practical applications. To compensate for these defects, they designed a symmetric key based authentication protocol for WMSNs environment using only computationally efficient operations to achieve lightweight attribute. Unfortunately, the authors find that all these schemes cannot achieve forward secrecy effectively.

Motivation and Contributions

User anonymity and forward secrecy are two indispensable security properties of the authentication scheme (Gope & Hwang, 2016), especially for some scenarios containing real-time sensitive data, such as health monitoring. If the long-term keys are obtained by an adversary, it may cause the disclosure of the session key used in previous communications. Further, the content of previous communications may be revealed. The adversary can access the patients’ physiological data and assess the patients’ health status, it is devastating for the patients’ privacy. To the best of our knowledge, none of the existing scheme can achieve user anonymity and forward secrecy at the same time. In particular, it is disturbing to find that forward security has not been considered even when designing authentication schemes (He et al., 2015; Li et al., 2016; Srinivas et al., 2017). In fact, forward secrecy is present in several major protocol implementations, such as SSH and IPsec. In addition, forward secrecy has also been seen as an important security feature and provided to users by several large internet information providers, such as Google, Twitter, Facebook and Apple. It is a consensus to take forward security into consideration in the design of an effective lightweight anonymous authentication scheme (Mir et al., 2017; Khan & Kumari, 2013; Jin et al., 2015). As a step towards this direction, in this paper,
the authors adopt pseudonym identity technique to protect healthcare professional’s real identity, and employ one-way hash chain technique (Gope & Hwang, 2016) to ensure forward secrecy. The contributions of this paper are summarized mainly as follows:

1. The authors present a novel and lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications using only the lightweight cryptographic primitives, which is easy to carry out in practical applications.
2. The authors use Burrows-Abadi-Needham (BAN) logic (Burrows, Abad, & Needham, 1989) to prove that the proposed scheme is secure and fulfills mutual authentication successfully.
3. The authors conduct a formal verification of the proposed scheme using the widely-accepted tool ProVerif (Burrows, 2001, pp. 82-96).
4. The security analysis shows that the proposed scheme can not only provide user anonymity and forward secrecy, but also resist various malicious attacks, such as smart card loss attack, replay attack and wrong password login attack.
5. The authors evaluate the performance of the proposed scheme with other related schemes, and the results show that the proposed scheme can reduce the computational cost substantially.

PRELIMINARY KNOWLEDGE

In this section, the authors briefly introduce security requirements for healthcare applications and adversary attack model.

Security Requirements for Healthcare Applications

Since the communications between the health professional and the medical sensor nodes are done via public channel, the designed authentication scheme must be secure and efficient. Here the authors describe some important requirements for a secure anonymous authentication scheme in WMSNs:

- **User anonymity:** The first indispensable attribute of the authentication scheme for WMSNs is user anonymity, which mainly comprises two properties. The first one is user identity-protection which means the real identity of the user cannot be figured out by the adversary. Untraceability is another important property, which guarantees the adversary neither determining who the user is nor telling apart whether two sessions are executed by the same user (Wang & Wang, 2014). Therefore, the anonymous authentication scheme is very crucial to address privacy problem in WMSNs.

- **Forward secrecy:** If the long-term keys used to generate the session key are obtained by an adversary, it may cause the disclosure of the session key used in previous communications. Further, the content of previous communications may be revealed. The adversary can access the patients’ physiological data and assess the patients’ health status, it is devastating for the patients’ privacy. Therefore, anonymous authentication scheme must achieve forward secrecy.

- **Mutual authentication:** Mutual authentication among the health professional, GWN and the medical sensor node is needed, it is an essential requirement for all authentication schemes.

- **Session key agreement:** After mutual authentication, further communications should be encrypted using the shared session key to achieve confidentiality. Therefore, the proposed scheme should provide session key agreement.

- **Attacks resistance:** To ensure secure communication, the designed authentication scheme is able to resist various attacks, liking smart card loss attack, replay attack and wrong password login attack.
Adversary Attack Model

In this paper, the authors propose an authentication scheme based on the Dolev-Yao threat model (Dolev & Yao, 1983), which is the most widely accepted attacker model in the analysis of security protocols. According to this model, any two communicating parties communicate over an insecure channel and the endpoint entities are not considered as trusted entities. Based on this threat model and real application environments, the abilities of an adversary $A$ are summarized as follows:

1. $A$ may be a legitimate but malicious health professional in WMSNs.
2. $A$ may be a legitimate but malicious medical sensor node.
3. $A$ can intercept and modify the transmitted messages over insecure public communication channel easily (Ameen et al., 2012).
4. $A$ can acquire all the secret values stored in the smart card using side-channel attacks (Kocher, Jaffe, & Jun, 1999).
5. $A$ can get the long-term secret keys when forward secrecy is evaluated.
6. $A$ is a probabilistic polynomial time attacker. That is to say, $A$ can guess the low-entropy password and identity information within polynomial time.
7. There is no tamper-resistant hardware equipped in medical sensor nodes. In other words, $A$ can extract all the sensitive data stored in medical sensor nodes.

THE PROPOSED SCHEME

In this section, the authors present a lightweight three-factor anonymous authentication scheme for personalized healthcare applications using WMSNs, which not only achieves the required security attributes, liking user anonymity and forward secrecy, but also withstands various attacks. The proposed scheme is divided into four phases: registration phase, login and authentication phase, password change phase. For ease of presentation, some intuitive abbreviations and notations mentioned in the proposed scheme are listed in Table 1.

Table 1. Notations

<table>
<thead>
<tr>
<th>Notation</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U$</td>
<td>Remote health professional</td>
</tr>
<tr>
<td>$GWN$</td>
<td>Gateway node</td>
</tr>
<tr>
<td>$SN_j$</td>
<td>Medical sensor node</td>
</tr>
<tr>
<td>$ID_i$</td>
<td>Unique identity of $U_i$</td>
</tr>
<tr>
<td>$PW_i$</td>
<td>Password of $U_i$</td>
</tr>
<tr>
<td>$fs_i$</td>
<td>Biometric information of $U_i$</td>
</tr>
<tr>
<td>$HID_i$</td>
<td>Pseudonym identity of $U_i$</td>
</tr>
<tr>
<td>$SID_j$</td>
<td>Unique identity of $SN_j$</td>
</tr>
<tr>
<td>$E_{[\cdot]}(\cdot)$</td>
<td>Symmetric encryption/decryption with key $k$</td>
</tr>
<tr>
<td>$R, R_i$</td>
<td>Random number</td>
</tr>
<tr>
<td>$T_i, T_2, T_3, T_4$</td>
<td>Current time stamp</td>
</tr>
<tr>
<td>$\Delta T$</td>
<td>The maximum of the transmission delay time</td>
</tr>
<tr>
<td>$K$</td>
<td>Secret key generated by GWN</td>
</tr>
<tr>
<td>$SK$</td>
<td>Session key</td>
</tr>
<tr>
<td>$h(\cdot)$</td>
<td>One-way hash function</td>
</tr>
<tr>
<td>$BH(\cdot)$</td>
<td>Biohash function</td>
</tr>
<tr>
<td>$\XOR$</td>
<td>Concatenate operation</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>XOR operation</td>
</tr>
</tbody>
</table>
Registration Phase

The registration phase is divided into two parts, i.e., health professional registration phase and medical sensor node registration phase.

Health Professional Registration

When a new health professional wants to be a legitimate user in WMSNs, he/she must register in GWN first. The procedure of professional’s registration is described as follows:

**Step 1:** The health professional $U_i$ chooses his/her identity $ID_i$, password $PW_i$ and imprints its biometrics $fg_i$ via a sensor, and generates a random number $m_i$. Then $U_i$ computes $MB_i = BH(m_i || f_{g_i})$, $MPW_i = h(ID_i || PW_i || MB_i || m_i)$, $U_i$ sends the message $\{ID_i, MPW_i\}$ and his/her personal credential to GWN through a secure channel.

**Step 2:** Upon receiving the message, GWN generates three random integers $n_i$, $r_i$, $K_i$ and computes $HID_i = ID_i \oplus r_i$, $X_i = h\{ID_i || K || n_i\}$, $Y_i = X_i \oplus MPW_i$, $V_i = h(X_i || MPW_i)$. After that, GWN stores $\{ID_i, HID_i, n_i, K_i\}$ into its own database and also maintains a health professional personal credential table. Finally, GWN writes $\{HID_i, Y_i, V_i, K_i, h(.), BH(.)\}$ into smart card and issues it to $U_i$ via a private channel.

**Step 3:** Upon receiving the smart card, $U_i$ writes $m_i$ into the smart card. Finally, the smart card contains $\{HID_i, Y_i, V_i, K_i, m_i, h(.), BH(.)\}$.

Medical Sensor Node Registration

The procedure of medical sensor node registration is outlined as follows:

**Step 1:** The medical sensor node $SN_j$ selects the identity $SID_j$ and transmits it to GWN via a secure channel.

**Step 2:** Upon receiving $SID_j$, GWN first checks whether $SID_j$ exists in the medical sensor node information table. If it exists, GWN refuses the medical sensor node registration request. Otherwise, GWN generates a random integer $K_2$ and stores $\{SID_j, K_2\}$ into its sensor node information table. After that, GWN sends $K_2$ to $SN_j$ via a private channel.

**Step 3:** Upon receiving the message from GWN, $SN_j$ stores $K_2$ into its memory secretly.

Login and Authentication Phase

When a health professional $U_i$ wants to access a medical sensor node, he/she needs to login in GWN first. As shown in Figure 2, the procedure of health professional’s login and authentication phase is described as follows:

**Step 1:** The health professional $U_i$ inserts his smart card into a card reader and inputs the identity $ID_i$, the password $PW_i$ and enters the fingerprint $fg_i$ at the sensor device. Then, the smart card computes $MB'_i = BH(m_i || f_{g_i})$, $MPW'_i = h(ID_i || PW_i || MB'_i || m_i)$, $X'_i = Y_i \oplus MPW'_i$, $V'_i = h(X'_i || MPW'_i)$, and compares $V'_i$ with the stored value $V_i$. If they are not equal, the smart card terminates the session. Otherwise, the smart card proceeds to the next step.

**Step 2:** After verifying the legitimacy of health professional $U_i$, the smart card generates a random number $R$ and gets the current time $T_i$. After that, $U_i$ selects the identity $SID_j$ of the medical sensor node $SN_j$ that he/she wants to access, and the smart card computes $UG = h(HID_j || X'_i || K_i)$,
M₀ = Eᵥ(R || S₀), CK₀ = h(ID₀ || R || X₀ || HID₀ || K₀ || T₀). Then U₀ sends the login message {HID₀, M₀, CK₀, T₀} to GWN through a public channel.

Step 3: Upon receiving the login request message, GWN first checks the validity of the time stamp T₀. If the matching score |T₀* - T₀| is beyond a predefined threshold value ΔT, GWN terminates the session. Then, GWN extracts ID₀, n₀, and K₀ from user information database corresponding to pseudonym identity HID₀. Next, GWN computes X₀ = h(ID₀ || K₀ || n₀), U₀ = h(HID₀ || X₀ || K₀). Then GWN computes CK₀ = h(ID₀ || X₀ || HID₀ || K₀ || T₀) and compares CK₀ with the received value CK₀. If they are not equal, GWN terminates the session. Otherwise, GWN believes the legitimacy of U₀. What’s more, GWN generates a random number T₁ and a session key SK₀ and computes M₁ = (SK₀ || ID₀) ⊕ h(K₀ || T₀) and sends the message {M₁, CK₁, T₁} to the sensor node SN₁ via open channel.

Step 4: Upon receiving the message {M₁, CK₁, T₁}, SN₁ first checks the validity of the time stamp |T₁ - T₀| < ΔT and then verifies the timestamp freshness of the message. Then, SN₁ computes CK₁ = h(ID₀ || X₀ || HID₀ || K₀ || T₀) and checks if CK₁ matches with the received CK₁. If it is satisfied, SN₁ generates a random number T₂ and computes CK₂ = h(SID₁ || ID₁ || SK || K₂ || T₂). Then SN₁ sends the message {CK₂, T₂} to GWN through a public channel.

Step 5: GWN first checks the freshness of the time stamp T₂ and computes CK₂ = h(SID₁ || ID₁ || SK || T₂). Then, the GWN checks whether CK₂ matches with the received CK₂. If it does not hold, GWN terminates the session. Otherwise, GWN generates two random numbers r₁, T₃ and computes

\[ H₀ = D₀(U₀), \quad CK₀ = h(ID₀ || X₀ || HID₀ || K₀ || T₀) \]

\[ M₀ = Eᵥ(R || S₀), \quad CK₀ = h(ID₀ || R || X₀ || HID₀ || K₀ || T₀). \]

Then U₀ sends the login message {HID₀, M₀, CK₀, T₀} to GWN through a public channel.

Step 3: Upon receiving the login request message, GWN first checks the validity of the time stamp T₀. If the matching score |T₀* - T₀| is beyond a predefined threshold value ΔT, GWN terminates the session. Then, GWN extracts ID₀, n₀, and K₀ from user information database corresponding to pseudonym identity HID₀. Next, GWN computes X₀ = h(ID₀ || K₀ || n₀), U₀ = h(HID₀ || X₀ || K₀). Then GWN computes CK₀ = h(ID₀ || X₀ || HID₀ || K₀ || T₀) and compares CK₀ with the received value CK₀. If they are not equal, GWN terminates the session. Otherwise, GWN believes the legitimacy of U₀. What’s more, GWN generates a random number T₁ and a session key SK₀ and computes M₁ = (SK₀ || ID₀) ⊕ h(K₀ || T₀) and sends the message {M₁, CK₁, T₁} to the sensor node SN₁ via open channel.

Step 4: Upon receiving the message {M₁, CK₁, T₁}, SN₁ first checks the validity of the time stamp |T₁ - T₀| < ΔT and then verifies the timestamp freshness of the message. Then, SN₁ computes CK₁ = h(ID₀ || X₀ || HID₀ || K₀ || T₀) and checks if CK₁ matches with the received CK₁. If it is satisfied, SN₁ generates a random number T₂ and computes CK₂ = h(SID₁ || ID₁ || SK || K₂ || T₂). Then SN₁ sends the message {CK₂, T₂} to GWN through a public channel.

Step 5: GWN first checks the freshness of the time stamp T₂ and computes CK₂ = h(SID₁ || ID₁ || SK || T₂). Then, the GWN checks whether CK₂ matches with the received CK₂. If it does not hold, GWN terminates the session. Otherwise, GWN generates two random numbers r₁, T₃ and computes
CK₄ = h(IDᵢ || SK || HIDᵢ || T₄). After that, GWN updates K₁, K₂, HIDᵢ with K₁ = h(Kᵢ), K₂ = h(K₂), HIDᵢ = HIDᵢ', respectively. Finally, GWN sends the message {M₃, CK₄, T₄} to Uᵢ through a public channel.

**Step 6:** Upon receiving the message from GWN, Uᵢ first checks the time stamp T₄. If T₄ is fresh, GWN computes \( GU = h(R || HIDᵢ || Xᵢ || Kᵢ) \), \( (SK || HIDᵢ' || SIDᵢ) = D_{gu}(M₃) \), \( CK₄' = h(IDᵢ || SK || HIDᵢ || T₄) \). Then, Uᵢ checks whether CK₄' matches with the received value CK₄. If it holds, Uᵢ updates K₁, HIDᵢ with K₁ = h(Kᵢ), HIDᵢ = HIDᵢ' and completes the authentication. Otherwise, Uᵢ fails to authenticate GWN.

**Password Change Phase**

If a health professional Uᵢ wants to change his/her password, he/she needs to run as follows:

**Step 1:** Uᵢ first inserts his/her smart card into a card reader and inputs the identity IDᵢ, the password PWᵢ and imprints its biometrics fgᵢ via a sensor device. Then, the smart card computes MBᵢ = BH(Œₗ, Œfgᵢ, Œfₜ), MPWᵢ = h(IDᵢ || PWᵢ || MBᵢ || mᵢ), Xᵢ = Yᵢ ⊕ MPWᵢ, Vᵢ' = h(Xᵢ || MBᵢ). Uᵢ compares Vᵢ with Vᵢ which is stored in the smart card. If they are not equal, the smart card rejects the password change request. Otherwise, the smart card believes the legitimacy of Uᵢ and allows Uᵢ to input a new password PWᵢ'.

**Step 2:** The smart card computes MPWᵢ' = h(IDᵢ || PWᵢ' || MBᵢ || mᵢ), Yᵢ' = Xᵢ ⊕ MPWᵢ', Vᵢ' = h(Xᵢ || MPWᵢ').

**Step 3:** At last, Yᵢ' and Vᵢ' are stored in the smart card to replace Yᵢ and Vᵢ, respectively.

**SECURITY ANALYSIS OF THE PROPOSED SCHEME**

In this section, the authors first analyze the proposed scheme using the widely-accepted BAN logic (Burrows et al., 1989). In addition, the authors conduct a formal verification of the proposed scheme with Proverif (Blanchet, 2001, pp. 82-96). Finally, the authors discuss the possible attacks on the proposed scheme.

**Authentication Proof Based on the BAN Logic**

The BAN logic (Burrows et al., 1989) is an efficient way to analyze the security of a protocol, which is widely-used in many works, such as (Odelu, Das, & Goswami, 2015; He, Kumar, Lee, & Sherratt, 2014). For convenience, all the notations used in the BAN logic are given in Table 2.

Some primary rules of BAN logic are as given below:

- **Message-meaning rule:**
  \[
  P \models P \overset{K}{\leftarrow} Q, P \triangleleft X_k \\
  \frac{P \models Q \sim X}{P \models Q \sim X}
  \]

- **Nonce-verification rule:**
  \[
  P \models \#(X), P \models Q \sim X \\
  \frac{P \models Q \models X}{P \models Q \models X}
  \]

- **Jurisdiction rule:**
  \[
  P \models Q \models X, P \models Q \models X \\
  \frac{P \models Q \models X}{P \models X}
  \]

- **Freshness-conjunctication rule:**
  \[
  P \models \#(X) \\
  \frac{P \models \#(X)}{P \models \#(X,Y)}
  \]
The proposed scheme should satisfy following four goals:

**Goal 1:** $U_i \equiv (U_i \leftarrow_{SK} SN_j)$

**Goal 2:** $U_i \equiv SN_j \equiv (U_i \leftarrow_{SK} SN_j)$

**Goal 3:** $SN_j \equiv (U_i \leftarrow_{SK} SN_j)$

**Goal 4:** $SN_j \equiv U_i \equiv (U_i \leftarrow_{SK} SN_j)$

First of all, messages exchanged in the proposed scheme are transformed into idealized forms as follows:

**Msg1:** $U_i \rightarrow GWN : < ID_i, SID_j, R, HID_i, T_1, U_i \leftarrow_{K_1} GWN >_{U_i \rightarrow_{S_1} GWN}$

**Msg2:** $GWN \rightarrow SN_j : < ID_i, SID_j, T_2 >_{GWN \rightarrow_{S_2} SN_j}$

**Msg3:** $SN_j \rightarrow GWN : < ID_i, SID_j, T_3 >_{SN_j \rightarrow_{S_3} GWN}$

**Msg4:** $GWN \rightarrow U_i : < ID_i, SID_j, HID_i, T_4 >_{GWN \rightarrow_{S_4} U_i}$

Second, some initial assumptions about the proposed scheme are listed below:

**A1:** $GWN \equiv \#(T_1)$

**A2:** $SN_j \equiv \#(T_2)$

**A3:** $GWN \equiv \#(T_3)$

**A4:** $U_i \equiv \#(T_4)$

**A5:** $U_i \equiv U_i \leftarrow_{K_1} GWN$

**A6:** $GWN \equiv U_i \leftarrow_{K_1} GWN$

**A7:** $SN_j \equiv SN_j \leftarrow_{K_1} GWN$

**A8:** $GWN \equiv SN_j \leftarrow_{K_1} GWN$

---

Table 2. Notations in BAN logic

<table>
<thead>
<tr>
<th>Notation</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P \triangleleft X$</td>
<td>Principal $P$ sees a statement $X$</td>
</tr>
<tr>
<td>$P \equiv X$</td>
<td>Principal $P$ believes a statement $X$</td>
</tr>
<tr>
<td>$P \Rightarrow X$</td>
<td>Principal $P$ has jurisdiction over statement $X$</td>
</tr>
<tr>
<td>$P \sim X$</td>
<td>Principal $P$ once said a statement $X$</td>
</tr>
<tr>
<td>$(X)$</td>
<td>Statement $X$ is fresh</td>
</tr>
<tr>
<td>$(X, Y)$</td>
<td>Statement $X$ or $Y$ is one part of statement $(X, Y)$</td>
</tr>
<tr>
<td>$X_k$</td>
<td>Statement $X$ is encrypted with the key $K$</td>
</tr>
<tr>
<td>$&lt;X&gt;_Y$</td>
<td>Statement $X$ is combined with statement $Y$</td>
</tr>
<tr>
<td>$(X)_k$</td>
<td>Statement $X$ is hashed with the key $K$</td>
</tr>
<tr>
<td>$P \leftarrow_{K} Q$</td>
<td>Principal $P$ and principal $Q$ communicate with the shared key $K$</td>
</tr>
</tbody>
</table>
Third, based on the BAN logic rules and assumptions, the main proofs are performed as follows. According to the Msg1, the authors get:

\[ S_1: GWN \leftarrow\leftarrow ID_j, SID_j, R, HID_i, T_1, U_i \xrightarrow{X_i} GWN \xrightarrow{U_i \rightarrow SN_j} \]

Based on assumption A6, S1 and message-meaning rule, the authors have:

\[ S_2: GWN \equiv U_i \equiv (ID_j, SID_j, R, HID_i, T_1, U_i \xrightarrow{X_i} GWN) \]

From A1 and freshness-conjuncatenation rule, the authors get:

\[ S_3: GWN \equiv \#(ID_j, SID_j, R, HID_i, T_1, U_i \xrightarrow{X_i} GWN) \]

From S3, S2 and nonce-verification rule, the authors get:

\[ S_4: GWN \equiv U_i \equiv (ID_j, SID_j, R, HID_i, T_1, U_i \xrightarrow{X_i} GWN) \]

According to the Msg2, the authors get:

\[ S_5: SN_j \leftarrow\leftarrow ID_j, SID_j, T_2 \xrightarrow{GWN \rightarrow SN_j} \]

From A7, S5 and message-meaning rule, the authors have:

\[ S_6: SN_j \equiv GWN \equiv (ID_j, SID_j, T_2) \]

From A2 and freshness-conjuncatenation rule, the authors get:

\[ S_7: SN_j \equiv \# < ID_j, SID_j, T_2 > \]

From S7, S6 and nonce-verification rule, the authors get:

\[ S_8: SN_j \equiv GWN \equiv < ID_j, SID_j, T_2 > \]

According to the Msg3, the authors get:

\[ S_9: GWN \leftarrow\leftarrow ID_j, SID_j, T_3 \xrightarrow{SN_j \rightarrow GWN} \]
From A8, S9 and message-meaning rule, the authors have:

S10: \( \text{GWN} \models \text{SN}_j \sim (ID_i, SID_j, T_3) \)

From A3 and freshness-conjunctenate rule, the authors get:

S11: \( \text{GWN} \models \#(ID_i, SID_j, T_3) \)

From S11, S10 and nonce-verification rule, the authors get:

S12: \( \text{GWN} \models SN_j \models (ID_i, SID_j, T_3) \)

According to the Msg4, the authors get:

S13: \( U_i \leftarrow ID_i, SID_j, HID_i, T_4 \rightarrow GWN \xrightarrow{K_i} U_i \)

From A5, S13 and message-meaning rule, the authors have:

S14: \( U_i \models \text{GWN} \sim \leftarrow ID_i, SID_j, HID_i, T_4 \)

From A4 and freshness-conjunctenate rule, the authors get:

S15: \( U_i \models \#(ID_i, SID_j, HID_i, T_4) \)

From S15, S14 and nonce-verification rule, the authors get:

S16: \( U_i \models \text{GWN} \models (ID_i, SID_j, HID_i, T_4) \)

From S12, S16 and the session key \( SK \), the authors have:

S17: \( U_i \models \text{SN}_j \models (U_i \xleftarrow{SK} \text{SN}_j) \) (Goal2)

From S4, S8 and the session key \( SK \), the authors have:

S18: \( \text{SN}_j \models U_i \models (U_i \xleftarrow{SK} \text{SN}_j) \) (Goal4)

From S17, A9 and jurisdiction rule, the authors have:

S19: \( U_i \models (U_i \xleftarrow{SK} \text{SN}_j) \) (Goal1)
From S18, A10 and jurisdiction rule, the authors have:

$$S_{N_j} \equiv (U_i \rightarrow_{SK} S_{N_j}) \text{ (Goal3)}$$

According to Goal1-Goal4, the authors conclude that the proposed scheme can achieve mutual authentication successfully.

### Formal Security Verification Using ProVerif

ProVerif (Blanchet, 2001, pp. 82-96) is a formal verification tool which is widely used in many works, such as (Xiong, Peng, Peng, Liang, & Liu, 2017; Jiang, Zeadally, Ma, & He, 2017). Privacy and security of authentication schemes can be verified by ProVerif which supports many cryptographic primitives, including digital signatures, hash functions, encryption, Diffie-Hellman key agreements, and so on. In this subsection, the authors use ProVerif to analyze the security of the proposed scheme.

First of all, the authors define two public channels and basic types of variables. Secondly, the authors model the cryptographic functions of the proposed scheme, and the secret keys, events and authentication queries are defined. Thirdly, the authors model the process of the health professional, GWN and the medical sensor node, respectively. Finally, the authors model the whole process of the proposed scheme. The execution codes of the proposed scheme are placed on GitHub (Shuai, 2018), and the simulation results with ProVerif version 1.96 are given in Figure 3.

The results demonstrate that the proposed scheme fulfills the secrecy of session key and achieves mutual authentication successfully.

### Figure 3. The simulation results with the ProVerif

Completing...
Starting query not attacker(snameA[])
RESULT not attacker(snameA[]) is true.
Starting query not attacker(snameB[])
RESULT not attacker(snameB[]) is true.
Starting query not attacker(snameC[])
RESULT not attacker(snameC[]) is true.
Starting query not attacker(snameD[])
RESULT not attacker(snameD[]) is true.
-- Query inj-event(SGend(x_2072)) ==> inj-event(SGbegin(x_2072))
Completing...
Starting query inj-event(SGend(x_2072)) ==> inj-event(SGbegin(x_2072))
RESULT inj-event(SGend(x_2072)) ==> inj-event(SGbegin(x_2072)) is true.
-- Query inj-event(GSend(x_4178)) ==> inj-event(GSbegin(x_4178))
Completing...
Starting query inj-event(GSend(x_4178)) ==> inj-event(GSbegin(x_4178))
RESULT inj-event(GSend(x_4178)) ==> inj-event(GSbegin(x_4178)) is true.
-- Query inj-event(GHend(x_6181)) ==> inj-event(GHbegin(x_6181))
Completing...
Starting query inj-event(GHend(x_6181)) ==> inj-event(GHbegin(x_6181))
RESULT inj-event(GHend(x_6181)) ==> inj-event(GHbegin(x_6181)) is true.
-- Query inj-event(HGend(x_8172)) ==> inj-event(HGbegin(x_8172))
Completing...
Starting query inj-event(HGend(x_8172)) ==> inj-event(HGbegin(x_8172))
RESULT inj-event(HGend(x_8172)) ==> inj-event(HGbegin(x_8172)) is true.
Analysis of Security Properties

In this section, the authors look at how the proposed scheme provides user anonymity, forward secrecy, mutual authentication, session key agreement, security against smart card loss attack and replay attack.

The Proposed Scheme Provides User Anonymity

In the proposed scheme, the authors adopt pseudonym identity technique to protect health professional’s real identity. The pseudonym identity generated randomly by GWN is updated during every session, so the transmitted messages in current session are also different from other session. In addition, the health professional’s real identity is protected by one-time hash function, the adversary cannot get it even if he/she intercept the transmitted messages. Therefore, the proposed scheme can not only protect the health professional’s real identity, but also provide untraceability.

The Proposed Scheme Provides Forward Secrecy

In the proposed scheme, even if an attacker obtains the long-term keys $K_1, K_2$ and $X_i$, he/she cannot get the session key which was used in previous communications. The reason is that the long-term keys $K_1^*$ and $K_2^*$ are updated by $K_1^* = h(K_1^*)$ and $K_2^* = h(K_2^*)$ after each session. The attacker cannot get $K_1^*$ and $K_2^*$ from $K_1$ and $K_2$ because hash function is irreversible. Therefore, the proposed scheme provides forward secrecy.

The Proposed Scheme Achieves Mutual Authentication

In the proposed scheme, mutual authentication between health professional and GWN will be achieved by checking $C_{K_1^*} = C_{K_1}$ and $C_{K_4^*} = C_{K_4}$. Similarly, mutual authentication between GWN and the medical sensor node will be achieved by checking $C_{K_2^*} = C_{K_2}$ and $C_{K_3^*} = C_{K_3}$. Therefore, the proposed scheme achieves mutual authentication successfully.

The Proposed Scheme Provides Session Key Agreement

In the execution of the proposed scheme, health professional, GWN and the medical sensor node establish a shared session key $SK$ to protect future communications in WMSNs. Therefore, the proposed scheme provides session key agreement.

The Proposed Scheme is Resistant to Smart Card Loss Attack

Suppose the smart card is lost/stolen, an attacker can get the stored secret values $\{HID_1, Y_i, V_i, K_j, m_i, h(.), BH(.), V h X P W_i, V h X P W_i, \}$, where $V_i = h \left( X_i \parallel MPW_i \right)$, $X_i = h \left( ID_i \parallel K \parallel n_i \right)$, $Y_i = X_i \oplus MPW_i$, $HID_i = ID_i \oplus r_i$, $MB_i = BH \left( m_i \parallel f_g_i \right)$, $MPW_i = h \left( ID_i \parallel PW_i \parallel MB_i \parallel m_i \right)$, $MB_i = BH \left( m_i \parallel f_g_i \right)$. Here, the authors also suppose that the transmitted messages via open channels can be eavesdropped by the attacker. Using these values, the attacker can launch a smart card loss attack and try to guess the health professional’s real identity and password. However, the attack will be failed without knowing the health professional’s personal biometric $f_g_i$, GWN’s secret key $K$ and the high entropy random integer $n_i$ generated by GWN. Therefore, the proposed scheme is resistant to smart card loss attack.

The Proposed Scheme Resists Replay Attack

The proposed scheme adopts the time stamp to avoid the replay attack. In the replay attack, an adversary cannot pass the time stamp checking process because all transmitted messages including current time stamp values, i.e., $T_1, T_2, T_3, T_4$. Therefore, the proposed scheme resists replay attack.
The Proposed Scheme Resists Wrong Password Login Attack

In the proposed scheme, the value $V_i$ stored in the smart card is used to verify the legality of health professional, where 

$$ V_i^* = h(X_i^* || MPW_i^+) $$

$$ X_i^* = Y_i \oplus MPW_i^* $$

$$ MPW_i^* = h(ID_i || PW_i || MB_i^* || m_i), \ MB_i^* = BH(m_i || f_g) $$

If the health professional inputs a wrong password $PW_i^*$, the values $V_i^*$ and $V_i$ will be not equal. At this moment, the smart card rejects the health professional’s login request. Therefore, the proposed scheme resists wrong password login attack.

PERFORMANCE ANALYSIS

In this section, the authors compare the computational costs of the proposed scheme with other related schemes (He et al., 2015; Li et al., 2016; Srinivas et al., 2017). In order to evaluate the computational costs, the authors define two computational notations $T_h$ and $T_{cr}$, where $T_h$ denotes the time complexity of a one-way hash function operation, and $T_{cr}$ denotes the time complexity of general symmetric-key encryption/decryption operation. According to the existing experimental results (He, Kumar, Lee, & Sherratt, 2014), the execution time of a one-way hash function operation and general symmetric-key encryption/decryption operation are 0.00032s and 0.0056s, respectively. The simulations are achieved on a machine characterized by a processing rate of 3.2 GHz and a memory of 4 GB, the results are averaged over 300 randomised simulation runs. The comparison results between the proposed scheme and other related schemes are shown in Table 3.

In WMSNs, medical sensor nodes are limited in terms of computation capabilities and thus, the user authentication scheme must be lightweight in terms of computation. The proposed scheme only uses the lightweight cryptographic primitives including one-way hash function and symmetric encryption/decryption algorithm, which are efficient. Although the proposed scheme increases the number of hash operations slightly, it reduces the number of symmetric encryption/decryption operations substantially. Comparison demonstrates that the proposed scheme performs better than He et al.’s scheme (He et al., 2015), Li et al.’s scheme (Li et al., 2016) and Srinivas et al.’s scheme (Srinivas et al., 2017). It is valuable to note that the proposed scheme achieves the required security attributes and is more suitable for personalized healthcare applications.

CONCLUSION

With the wide use of WMSNs in healthcare applications, security and privacy issues have become a great challenge. In order to securely transmit physiological data collected from patients, the authors propose a novel and lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications using only the lightweight cryptographic primitives. Using

![Table 3. Performance comparison between the proposed scheme and other related schemes](attachment:table3.png)
the BAN logic, the authors have proved that the proposed scheme fulfills mutual authentication successfully. In addition, the authors evaluated the security of the proposed scheme with ProVerif, and the simulation results show that the proposed scheme is secure. Through the heuristic way, the authors prove that the proposed scheme can not only provide user anonymity and forward secrecy, but also resist various malicious attacks, such as smart card loss attack and replay attack. Finally, the authors evaluate the performance of the proposed scheme with other related schemes, and the results show that the proposed scheme reduces the computational cost substantially and is more suitable for personalized healthcare applications.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (NSFC) under the grant No. U1536110.
REFERENCES


Mengxia Shuai received the B.S. and M.S. degrees from Fuzhou University, Fuzhou, China. Currently, he is pursuing the Ph.D. degree at University of Science and Technology of China. His research interests include cryptography and information security.

Nenghai Yu received his B.S. degree in 1987 from Nanjing University of Posts and Telecommunications, M.E. degree in 1992 from Tsinghua University and Ph.D. degree in 2004 from University of Science and Technology of China, where he is currently a professor. His research interests include multimedia security, multimedia information retrieval, video processing, information hiding and security, privacy, and reliability in cloud computing.

Hongxia Wang received the B.S. degree from Hebei Normal University, Shijiazhuang, China, in 1996, and the M.S. and Ph.D. degrees from University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2002, respectively. She pursued post-doctoral research with Shanghai Jiao Tong University, Shanghai, China, from 2002 to 2004 and was a Visiting Scholar with Northern Kentucky University, Highland Heights, KY, USA, from 2013 to 2014. She is currently a Professor with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu. She has authored over 100 research papers in refereed journals and conferences, and holds 10 authorized patents. Her research interests include multimedia information security, digital forensics, information hiding, and digital watermarking.

Ling Xiong received the M.S. degree from Southwest Jiaotong University, Chengdu, China. She is currently pursuing the Ph.D. degree in the school of information science and technology of Southwest Jiaotong University. Her research interests include the formal analysis of cryptographic protocol, the security and privacy in cloud computing services environment and wireless sensor networks environment.

Yue Li received the B.S. degree from Southwest Jiaotong University, Chengdu, China. Now she is pursuing the Ph.D. degree in the school of information science and technology of Southwest Jiaotong University. Her research interests include multimedia information security, information hiding, and digital watermarking.