Multimedia Systems (2015) 21:49–60
DOI 10.1007/s00530-013-0346-9

REGULAR PAPER

Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks

Debiao He · Neeraj Kumar · Jianhua Chen · Cheng-Chi Lee · Naveen Chilamkurti · Seng-Soo Yeo

Published online: 10 December 2013

Abstract With the fast development of wireless communication technologies and semiconductor technologies, the wireless sensor network (WSN) has been widely used in many applications. As an application of the WSN, the wireless medical sensor network (WMSN) could improve health-care quality and has become important in the modern medical system. In the WMSN, physiological data are collected by sensors deployed in the patient's body and sent to health professionals' mobile devices through wireless communication. Then health professionals could get the status of the patient anywhere and anytime. The data collected by sensors are very sensitive and important. The leakage of them could compromise the patient's privacy and their malicious modification could harm the patient's health. Therefore, both security and privacy are two important issues in WMSNs. Recently, Kumar et al. proposed an efficient authentication protocol for health-care applications using WMSNs and claimed that it could withstand various attacks. However, we find that their protocol is vulnerable to the off-line password guessing attack and the privileged insider attack. We also point out that their protocol cannot provide user anonymity. In this paper, we will propose a robust anonymous authentication protocol for health-care applications using WMSNs. Compared with Kumar et al.'s protocol, the proposed protocol has strong security and computational efficiency. Therefore, it is more suitable for health-care applications using WMSNs.

Keywords Wireless medical sensor network · Authentication protocol · Smart card

D. He · J. Chen
School of Mathematics and Statistics, Wuhan University, Wuhan, China

D. He
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

N. Kumar
Department of Computer Science and Engineering, Thapar University, Patiala, India
e-mail: neeraj.kumar@thapar.edu

C.-C. Lee
Department of Library and Information Science, Fu Jen Catholic University, New Taipei, Taiwan

N. Chilamkurti (✉)
Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia
e-mail: n.chilamkurti@latrobe.edu.au

S.-S. Yeo
Mokwon University, Daejeon, Korea

1 Introduction

With the development of technological advances in wireless communication, low-power integrated circuits and sensors, the wireless sensor network (WSN) has been widely used in many fields such as environmental testing, military detection, industry control, health care and so on. Because of its brighter prospect in many applications, WSN attracts more and more attention from the academia and industry. As an important application of WSN, the wireless medical sensor network (WMSN) also receives a great deal of attention. A WMSN is a concrete WSN network, which comprises many lightweight devices with limited memory, limited computing power and limited bandwidth. First, many medical sensors are fixed on the

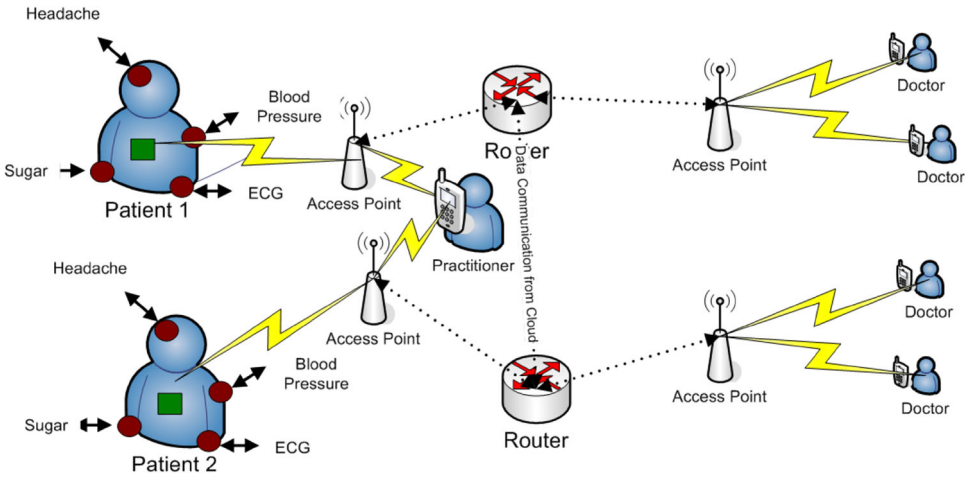

Fig. 1 WMSN in a hospital environment

patients' body. Then, those sensors collect patients' physiological such as heartbeat rates, pulse, temperature and so on. Health professionals may obtain real-time health-care monitoring through the wireless using handheld devices. Figure 1 [1] demonstrates a typical architecture of the WMSN used in the hospital environment.

The collected medical data over WMSNs is very sensitive, since the leakage of those data may invade patients' privacy and the modification of those data may result in an improper diagnosis or treatment. Therefore, it is very important to guarantee secure communication in WMSNs. Based on previous work [1–9], the functionality requirements of the WMSN for health-care application are listed as follows.

Mutual authentication Mutual authentication protocol for WMSNs allows the health professional, the gateway and the sensor to authenticate each other.

Session key establishment Session key establishment means that a session key is generated in the authentication protocol. The session key will be used to protect future communications.

Known-key security Known-key security means that the adversary cannot get session keys in other sessions when he gets a session key in some session.

Low communication and computational cost The memory, computing power and bandwidth of sensors are very limited. The authentication protocol for WMSNs should have low communication and computation cost.

User friendliness The user could choose his identity and password freely. Besides, he could update his password securely and freely.

User anonymity The adversary cannot get the identities of health professionals and the patients.

Secure against various attacks The authentication protocol could withstand popular attacks, such as password guessing attack, replay attack, stolen verifier table attack, stolen smart card attack, privileged insider attack, man-in-the-middle attack and impersonation attack.

Many authentication protocols for WMSNs have been proposed for medical applications. Malasri and Wang [7] presented an efficient WMSN system for health-care applications. They use a secure key agreement scheme based on elliptic curve cryptography (ECC) to generate a session key. They also use a secure symmetric encryption algorithm to ensure confidentiality and integrity of data collected by medical sensors. Hu et al. [8] proposed a real-time cardiac patient health-care monitoring system for the US health-care society. They also use a symmetric encryption algorithm to protect privacy and ensure secure communication in WMSNs. Hu et al.'s system could protect patients' privacy. However, their system could not solve the strong user authentication effectively. Later, Le et al. [9] presented a mutual authentication protocol using ECC. Le et al. claimed that their scheme could withstand various attacks and provide user anonymity. However, their protocol is vulnerable to the information-leakage attack since a malicious user could get other users' vital signals. Huang et al. [10] presented a hierarchical health-care monitoring architecture for WMSNs. They used the Advanced Encryption Standard (AES) Algorithm to provide authentication and encryption. However, mutual authentication is not considered in their architecture. Therefore, Huang et al.'s architecture is not practical enough.

Das [11] presented an authentication protocol for WSNs and claimed their protocol could withstand various attacks. His protocol is very efficient, since only hash function operation is required. However, Nyang and Lee [12] pointed out that Das's protocol cannot withstand the sensor node compromising attack and the off-line password guessing attack. Huang et al. [13] also found that Das's protocol could not withstand the impersonation attack. Chen and Shih [14] found that Das's protocol could not provide mutual authentication. Khan and Alghathbar [15] demonstrated that Das's protocol could not withstand the

privileged insider attack and the gateway node bypassing attack. Chen and Shih [14] and Khan and Alghathbar [15] also proposed an improved authentication protocol separately. However, Yoo et al. [16] pointed out that Chen et al.'s protocol was vulnerable to the impersonation attack and the replay attack. They also pointed out that Khan and Alghathbar's protocol could not provide mutual authentication. Yeh et al. [17] used ECC to design a new authentication protocol for WSNs. Unfortunately; Han [18] demonstrated that mutual authentication could not be provided in their scheme. To solve the problem, Shi and Gong [19] used ECC to construct a new authentication protocol for WSNs. ECC is used in Yeh et al.'s protocol and Shi and Gong's protocol, it not only increases computational complexity, but also requires additional storage to store sensor nodes and users' public keys. Therefore, they are not suitable for health-care applications using WMSNs. Very recently, Kumar et al. [1] presented a new authentication protocol for WMSNs and claimed that it could satisfy all security requirements in WMSNs. However, we find that Kumar et al.'s protocol cannot withstand the privileged insider attack and the off-line password guessing attack. Besides, we also demonstrate that Kumar et al.'s protocol cannot provide the user anonymity. To improve security, we propose a new anonymous authentication protocol for WMSNs.

The organization of the paper is described as follows. Section 2 reviews Kumar et al.'s protocol briefly. The security of Kumar et al.'s protocol is analyzed in Sect. 3. Section 4 proposes a new anonymous authentication protocol for health-care applications using WMSNs. Security analysis and performance analysis will be given in Sects. 5 and 6 separately. Some conclusions are proposed in Sect. 7.

2 Review of Kumar et al.'s protocol

Kumar et al.'s authentication protocol is reviewed briefly in this section. For convenience, some notations used in the paper are defined as follows.

- U_i: the ith health professional;
- PW_i: the password U_i;
- ID_i: the identity of U_i;
- ID_{pt}: the identity of the patient;
- GW: the gateway node;
- ID_g: the identity of GW;
- S_n: the sensor node;
- J, K, Q: three secret keys of GW;
- $E_{key}[\cdot]$: the symmetric encryption algorithm using key key;
- $D_{key}[\cdot]$: the symmetric decryption algorithm using key key;
- $h(\cdot)$: a secure hash function;
- $\|$: the concatenation operation.

There are four phases in Kumar et al.'s protocol, i.e., the professional registration phase, the patient registration phase, the login and authentication phase and the password-change phase. Also, the following assumptions hold in their protocol.

1. The hospital registration center is a trusted authority.
2. The gateway node has three 256 bits secret keys, i.e., J, K and Q.
3. The sensor node and the gateway node share a secret key $SK_{gs} = h(ID_g||Q)$.

2.1 Professional registration phase

The health professional U_i becomes a legal user of the WNSN by registering in the gateway node GW through the following steps:

1. U_i sends his ID_i and password PW_i to GW through a secure channel.
2. Upon receiving the identity ID_i and the password PW_i, GW computes $C_{ig} = E_J[ID_i||ID_g]$ and $N_i = h(ID_i \oplus PW_i \oplus K)$, where K is GW's secret key. Then GW stores $\{h(\cdot), C_{ig}, N_i, K\}$ into a smart card and delivers it to U_i.

2.2 Patient registration phase

To enjoy health-care applications, the patient should register in the hospital registration center through the following steps:

1. The patient sends his name to the registration center.
2. The registration center chooses a suitable sensor kit and designates professionals.
3. The registration center sends the patient's identity ID_{pt} and information of medical sensors to the designated professionals.

2.3 Login and authentication phase

As shown in Fig. 2, a health professional U_i could access the patients' physiological information from the WMSN through the following steps:

1. U_i inserts his smart card into a card reader and inputs ID_i and PW_i. The smart card computes $N_i^* = h(ID_i \oplus PW_i \oplus K)$ and checks whether N_i^* and N_i are equal. If they are not equal, the smart cared rejects the request; otherwise, the smart card chooses a random

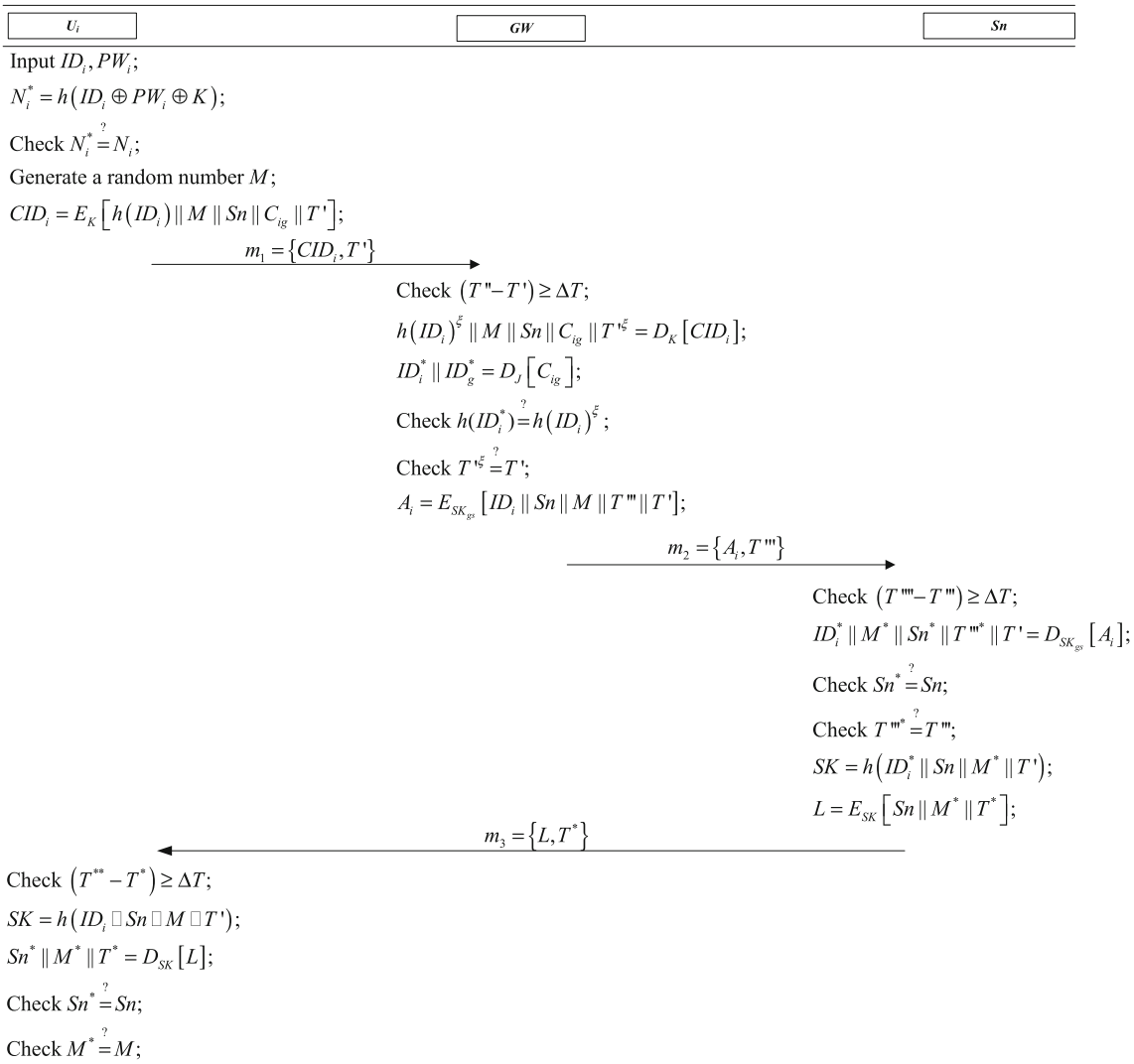

Fig. 2 Login and authentication phase of Kumar et al.'s protocol

number M and computes $CID_i = E_K[h(ID_i)||M||Sn||C_{ig}||T']$, where T' is the current timestamp. At last, the smart card sends the message $m_1 = \{CID_i, T'\}$ to GW.

2. Upon receiving m_1, GW checks whether the inequation $(T'' - T') \geq \Delta T$ holds, where ΔT is the permissible time limit for transmission delay and T'' is the current timestamp. If it holds, GW rejects the session; otherwise, GW uses K to decrypt CID_i and get $h(ID_i)^{\xi}$, M, Sn, C_{ig} and T'^{ξ}. GW uses J to decrypt C_{ig} and get ID_i^* and ID_g^*. GW checks whether T'^{ξ}, $h(ID_i)^{\xi}$ and ID_g^* equal T', $h(ID_i^*)$ and ID_g separately. If one of them is not equal, GW stops the session; otherwise, GW computes $A_i = E_{SK_{gs}}[ID_i||Sn||M||T'''||T']$, where T''' is the current timestamp. Then GW sends the message $m_2 = \{A_i, T'''\}$ to S_n.
3. Upon receiving m_2, S_n checks whether the inequation $(T'''' - T''') \geq \Delta T$ holds, where T'''' is the system's current timestamp and ΔT is the permissible time limit for transmission delay. If it holds, S_n stops the session; otherwise, S_n uses SK_{gs} to decrypt A_i and get ID_i^*, M^*, Sn^*, T'''^* and A. S_n checks whether Sn^* and T'''^* equal Sn and T''' separately. If either of them does not hold, S_n stops the session; otherwise, S_n computes $SK = h(ID_i^*||Sn||M^*||T')$ and $L = E_{SK}[Sn||M^*||T^*]$, where T^* is the current timestamp. At last, S_n sends the message $m_3 = \{L, T^*\}$ to the health professional U_i.
4. Upon receiving m_3, U_i checks whether the inequation $(T^{**} - T^*) \geq \Delta T$ holds, where T^{**} is the current time and ΔT is the permissible time limit for transmission delay. If it does not hold, U_i rejects the session; otherwise, U_i computes $SK = h(ID_i||Sn||M||T')$. Then U_i uses SK it to decrypt L and get M^* and Sn^*. Then U_i

checks whether M^* and Sn^* equal M and Sn separately. If either of them does not hold, U_i stops the session; otherwise U_i thinks that Sn is a legal one. Then U_i could access the patients' physiological information from WMSNs.

2.4 Password-change phase

When a health professional U_i wants to change his password, he will carry out the following steps:

1. U_i inserts his smart card into a card reader and inputs ID_i and PW_i. The smart card computes $N_i^* = h(ID_i \oplus PW_i \oplus K)$ and checks whether N_i^* and N_i are equal. If N_i^* and N_i are not equal, the smart card rejects the request.
2. U_i inputs a new password PW_i^{new} and replaces N_i with N_i^{new}, where $N_i^{new} = h\left(ID_i \oplus PW_i^{new} \oplus K\right)$.

3 Security analysis of Kumar et al.'s protocol

Kumar et al. claimed that their protocol could withstand various attacks. However, in this section, we will show that their protocol cannot withstand the off-line password guessing attack and the privileged insider attack. We also show that their protocol cannot provide user anonymity.

In the login and authentication phase of Kumar et al's protocol, all messages are sent through the public network. Then we can assume that an adversary can control the communication channel totally, i.e., he can intercept, insert, delete or interpolate any messages at his will.

3.1 Off-line password guessing attack

Previous work [20, 21] demonstrated that all smart cards were vulnerable to side channel attack, i.e., we could extract all confidential information stored in the smart cards through monitoring their power consumption. Then we could assume that the adversary A could extract the information stored in a health professional U_i's smart card. The off-line password guessing attack against Kumar et al.'s protocol is described as follows:

1. A steals the smart card of U_i.
2. A extracts the information $\{C_{ig}, N_i, K\}$ stored in the smart card through side channel attack, where $N_i = h(ID_i \oplus PW_i \oplus K)$ and $C_{ig} = E_J[ID_i||ID_g]$.
3. A guesses an identity ID_i^* and a password PW_i^*.
4. A computes $N_i^* = h\left(ID_i^* \oplus PW_i^* \oplus K\right)$ and checks whether N_i^* and N_i are equal. If N_i^* and N_i are equal, PW_i^* is the correct password; otherwise, A will repeat steps (3) and (4) until he finds the correct password.

In practical applications, people would like to choose easy-to-remember identity and password for convenience [22, 23]. Both identity and password must come from a very small dictionary. Therefore, A could find the correct identity and password through the brute-force attack. In most cases, the user would like to write his identity on his smart card. Then, A could get the user's identity when A steals the smart card. In this case, A just needs to guess the password. Therefore, the attack is available and Kumar et al.'s protocol is vulnerable to the off-line password guessing attack [24, 25].

3.2 Privileged insider attack

In practical environment, many users would like to choose the same password to access different applications to avoid remembering too many passwords [22, 23]. However, if a privileged insider A of the gateway node could get a health professional U_i's password, he may impersonate U_i to access other applications where U_i has registered as a legal user. In the professional registration phase of Kumar et al.'s protocol, U_i sends his identity ID_i and password PW_i to GW in plaintext format. A could get them easily. Therefore, Kumar et al.'s protocol cannot withstand the privileged insider attack [23].

3.3 User anonymity

Suppose that A gets a smart card of a health professional U_i. Then he could extract the information $\{C_{ig}, N_i, K\}$ stored in the smart card through side channel attack [20, 21], where $N_i = h(ID_i \oplus PW_i \oplus K)$ and $C_{ig} = E_J[ID_i||ID_g]$. With the information, A could get U_i's identity as follows:

1. A intercepts a message $m_1 = \{CID_i, T'\}$ sent by U_i, where T' is the current timestamp and $CID_i = E_K\left[h(ID_i)||M||Sn||C_{ig}||T'\right]$.
2. A uses K to decrypt CID_i and gets $h(ID_i)^{\xi}$, M, Sn, C_{ig} and T'^{ξ}.
3. A guesses an identity ID_i^* and computes $h(ID_i^*)$.
4. A checks whether $h(ID_i^*)$ and $h(ID_i)^{\xi}$ are equal. If $h(ID_i^*)$ and $h(ID_i)^{\xi}$ are equal, ID_i^* is the correct identity; otherwise, A repeats steps (3) and (4) until he finds the correct identity.

From the above description, we know that A can get U_i's identity. Therefore, Kumar et al.'s protocol cannot provide user anonymity as they claimed.

4 Our protocol

To overcome the weaknesses in Kumar et al.'s protocol, we propose a new anonymous authentication protocol for

WMSNs. Like Kumar et al.'s protocol, our protocol also consists of four phases, i.e., the professional registration phase, the patient registration phase, the login and authentication phase and the password-change phase. We also assume that the following assumptions hold:

1. The hospital registration center is a trusted authority.
2. The gateway node has three 256 bits secret keys, i.e., J, K and Q.
3. The sensor node and the gateway node have a shared key $SK_{gs} = h(ID_g||Q)$.

4.1 Professional registration phase

In this phase, the health professional U_i become a legal user of the WNSN by registering in the gateway node GW through the following steps:

1. U_i chooses ID_i and PW_i. Then, U_i chooses a random number r_i and sends ID_i and $h(PW_i||r_i)$ to GW securely.
2. Upon receiving ID_i and $h(PW_i||r_i)$, GW generates a random number r_g and computes $C_{ig} = E_J[r_g||ID_i||ID_g]$ and $N_i = h(ID_i||ID_g||K) \oplus h(PW_i||r_i)$, where K is GW's secret key. Then GW stores $\{h(\cdot), C_{ig}, N_i\}$ into a smart card and sends it to U_i securely.
3. Upon receiving the smart card, U_i inserts the random number r_i into it and finishes the registration. Then the smart card contains the information $\{h(\cdot), r_i, C_{ig}, N_i\}$.

4.2 Patient registration phase

To enjoy health-care applications, the patient should register in the hospital registration center through the following steps:

1. The patient sends his name to the registration center.
2. The registration center chooses a suitable sensor kit and designates professionals.
3. The registration center sends the patient's identity ID_{pt} and information of medical sensors to the designated professionals.

4.3 Login and authentication phase

As shown in Fig. 3, a health professional U_i could access the patients' physiological information from the WMSN through the following steps:

1. U_i inserts his smart card into a card reader and inputs ID_i and PW_i. The smart card chooses two random numbers M and N, and computes $CID_i = E_{N_i^*}[h(ID_i||C_{ig}||Sn||M||N||T')||Sn||M||N]$, where T' is the current timestamp and $N_i^* = N_i \oplus h(PW_i||r_i)$. Lastly, the smart card sends the message $m_1 = \{C_{ig}, CID_i, T'\}$ to GW.
2. Upon receiving $m_1 = \{C_{ig}, CID_i, T'\}$, GW checks whether the inequation $(T'' - T') \geq \Delta T$ holds, where ΔT is the permitted time limit for transmission delay and T'' is the current timestamp. If it holds, GW rejects the session; otherwise, GW computes $(r_g^\xi||ID_i^\xi||ID_g^\xi) = D_J[C_{ig}]$, $N_i^{*\xi} = h(ID_i^\xi||ID_g^\xi||K)$ and $(h^\xi||Sn^\xi||M^\xi||N^\xi) = D_{N_i^{*\xi}}[CID_i]$. GW checks whether h^ξ and $h(ID_i^\xi||C_{ig}||Sn^\xi||M^\xi||N^\xi||T')$ are equal. If they are not equal, GW rejects U_i's request; otherwise, GW generates a random number r_g^ξ and computes $C_{ig}^\xi = E_J[r_g^\xi||ID_i||ID_g]$, where $B_i = E_N(C_{ig}^\xi||N_i^{*\xi})$ and T''' is the current timestamp. Then GW sends the message $m_2 = \{A_i, T'''\}$ to S_n.
3. Upon receiving $m_2 = \{A_i, T'''\}$, S_n checks whether the inequation $(T'''' - T''') \geq \Delta T$ holds, where T'''' is the system's current timestamp and ΔT is the permissible time limit for transmission delay. If it holds, S_n stops the session; otherwise, S_n computes $(ID_i^*||Sn^*||M^*||B_i^*||T'''^*) = D_{SK_{gs}}[A_i]$. S_n checks whether Sn^* and T'''^* equal Sn and T''' separately. If either of them does not hold, S_n rejects the session; otherwise, S_n computes the session key $SK = h(ID_i^*||Sn||M^*||T'||T^*)$ and $L = E_{SK}[Sn||B_i^*||T^*]$, where T^* is the current timestamp. At last, S_n sends the message $m_3 = \{L, T^*\}$ to U_i.
4. Upon receiving $m_3 = \{L, T^*\}$, U_i checks whether the inequation $(T^{**} - T^*) \geq \Delta T$ holds, where T^{**} is the system's current time and ΔT is the permissible time limit for transmission delay. If it holds, U_i rejects the session; otherwise, U_i computes the session key $SK = h(ID_i||Sn||M||T'||T^*)$. Then U_i computes $(Sn^\xi||B_i^{*\xi}||T^{*\xi}) = D_{SK}[L]$ and checks whether $T^{*\xi}$ and T^* are equal. If $T^{*\xi}$ and T^* are not equal, U_i rejects the session; otherwise U_i computes $(C_{ig}^{\xi*}||h^\xi) = E_N(B_i^{*\xi})$ and checks whether h^ξ and $h(C_{ig}^{\xi*}||N_i^*)$ are equal. If they are not equal, U_i rejects the session; otherwise, U_i thinks that Sn is a legal one. Then U_i replaces C_{ig} with $C_{ig}^{\xi*}$ and gets the patients' physiological information from the WMSN.

4.4 Password-change phase

When a health professional U_i wants to change his password, he will carry out the following steps:

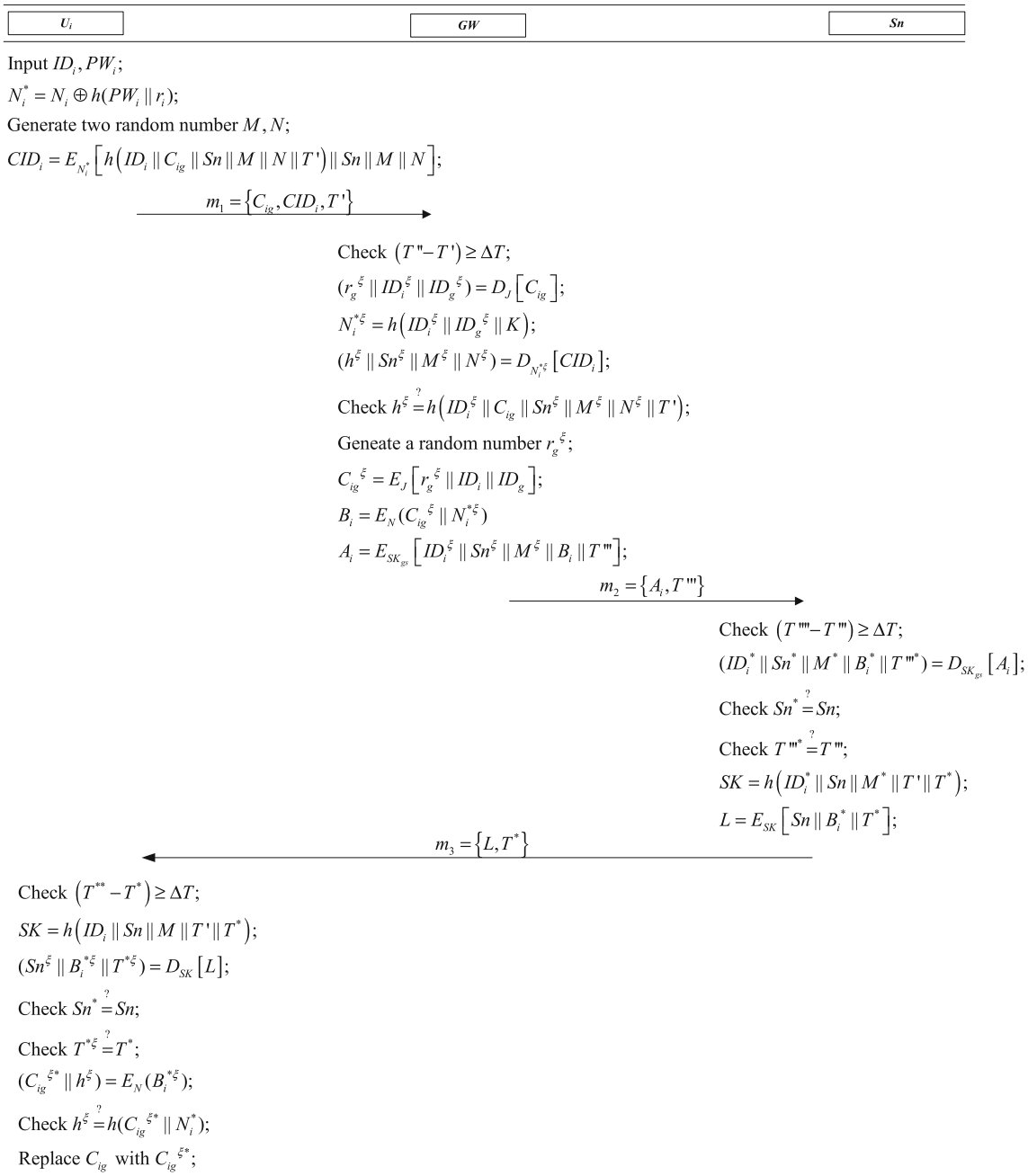

Fig. 3 Login and authentication phase of our protocol

1. U_i inserts his smart card into a card reader and inputs the identity ID_i, the old password PW_i and a new password PW_i^{new}.
2. U_i computes $N_i^{new} = N_i \oplus h(PW_i||r_i) \oplus h(PW_i^{new}||r_i)$ and replaces N_i with N_i^{new}.

5 Security analysis of our protocol

In this section, we will analyze the security of our authentication protocol for WMSNs. First, we will use the BAN logic [26, 27] to demonstrate the validity of our protocol. Then we will show that our protocol can satisfy security requirements in WMSNs.

5.1 Authentication proof based on the BAN logic

For convenience, we first give the description of some notations used in the BAN logic analysis.

- $P| \equiv X$: The principal P believes a statement X, or P is entitled to believe X.
- $\#(X)$: The formula X is fresh.

- $P \Rightarrow X$: The principal P has jurisdiction over the statement X.
- PX: The principal P sees the statement X.
- $P|\sim X$: The principal P once said the statement X.
- (X, Y): The formula X or Y is one part of the formula (X, Y).
- $\langle X \rangle_Y$: The formula X combined with the formula Y.
- $\{X\}_Y$: The formula X is encrypted under the key K.
- $(X)_Y$: The formula X is hash with the key K.
- $P \overset{K}{\leftrightarrow} Q$: The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q.
- SK: The session key used in the current session.

We also define some main logical postulates of BAN logic as follows, since they will be used in our proof.

- The message-meaning rule: $\frac{P \models P \overset{K}{\leftrightarrow} Q, P\{X\}_K}{P \models Q|\sim X}$.
- The freshness-conjuncatenation rule: $\frac{P \models \#(X)}{P \models \#(X,Y)}$.
- The nonce-verification rule: $\frac{P \models \#(X), P \models Q|\sim X}{P \models Q \models X}$.
- The jurisdiction rule: $\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$.

According to analytic procedures of BAN logic and the requirement of authentication protocol for WMSNs, our protocol should satisfy the following goals:

Goal 1. $U_i| \equiv (U_i \overset{SK}{\leftrightarrow} S_n)$;

Goal 2. $U_i| \equiv S_n| \equiv (U_i \overset{SK}{\leftrightarrow} S_n)$;

Goal 3. $S_n| \equiv (U_i \overset{SK}{\leftrightarrow} S_n)$;

Goal 4. $S_n| \equiv U_i| \equiv (U_i \overset{SK}{\leftrightarrow} S_n)$.

First of all, we transform the process of our protocol to the following idealized form.

$$CID_i = E_{N_i^*}\left[h\left(ID_i||C_{ig}||Sn||M||N \parallel T'\right)||Sn \parallel M||N\right]$$

$Msg1$.

$$U_i \rightarrow GW : \{ID_i, C_{ig}, Sn, U_i \overset{M}{\leftrightarrow} S_n, N, T'\}_{U_i \overset{h(ID_i||ID_g||K)}{\leftrightarrow} GW}$$

$Msg2$.

$$GW \rightarrow S_n : \{ID_i, Sn, U_i| \equiv (U_i \overset{M}{\leftrightarrow} S_n), B_i, T'''\}_{GW \overset{SK_{gs}}{\leftrightarrow} S_n}$$

$Msg3$. $S_n \rightarrow U_i : \{Sn, B_i, M, T*\}_{U_i \overset{SK}{\leftrightarrow} S_n}$.

According to the description of our protocol, we could make the following assumptions about the initial state, which will be used in the analysis of our protocol.

$A_1 : U| \equiv \#(M)$;

$A_2 : U| \equiv \#(T^*)$;

$A_3 : U_i| \equiv (U_i \overset{h(ID_i||ID_g||K)}{\leftrightarrow} GW)$;

$A_4 : U_i| \equiv S_n| \Rightarrow (U_i \overset{SK}{\leftrightarrow} S_n)$;

$A_5 : GW| \equiv \#(T')$;

$A_6 : GW| \equiv (U_i \overset{h(ID_i||ID_g||K)}{\leftrightarrow} GW)$;

$A_7 : GW| \equiv (S_n \overset{SK_{gs}}{\leftrightarrow} GW)$;

$A_8 : S_n| \equiv \#(T''')$;

$A_9 : S_n| \equiv (S_n \overset{SK_{gs}}{\leftrightarrow} GW)$;

$A_{10} : S_n| \equiv GW| \Rightarrow U_i| \equiv (U_i \overset{M}{\leftrightarrow} S_n)$;

$A_{11} : S_n| \equiv U_i| \Rightarrow (U_i \overset{SK}{\leftrightarrow} S_n)$.

Based on the above assumptions, the idealized form of our protocol is analyzed as follows. The main steps of the proof are described as follows:

According to the message $Msg1$, we could get:

$$S_1 : GW\{ID_i, C_{ig}, Sn, U_i \overset{M}{\leftrightarrow} S_n, N, T'\}_{U_i \overset{h(ID_i||ID_g||K)}{\leftrightarrow} GW}$$

According to A_6, we could get the following statement by applying the message-meaning rule to S_1:

$$S_2 : GW| \equiv U_i| \sim (ID_i, C_{ig}, Sn, U_i \overset{M}{\leftrightarrow} S_n, N, T').$$

According to A_5, we could get the following statement by applying the freshness-conjuncatenation rule to S_2:

$$S_3 : GW| \equiv U_i| \equiv (ID_i, C_{ig}, Sn, U_i \overset{M}{\leftrightarrow} S_n, N, T').$$

We could get the following statement by applying the BAN logic rule to break conjunctions rule to S_3:

$$S_4 : GW| \equiv U_i| \equiv (U_i \overset{M}{\leftrightarrow} S_n)$$

According to the message $Msg2$, we could get:

$$S_5 : S_n\{ID_i, Sn, U_i| \equiv (U_i \overset{M}{\leftrightarrow} S_n), B_i, T'''\}_{GW \overset{SK_{gs}}{\leftrightarrow} S_n}$$

According to A_9, we could get the following statement by applying the message-meaning rule to S_5:

$$S_6 : S_n \equiv GW| \sim \{ID_i, Sn, U_i| \equiv (U_i \overset{M}{\leftrightarrow} S_n), B_i, T'''\}.$$

According to A_8, we could get the following statement by applying the freshness-conjuncatenation rule to S_6:

$$S_7 : S_n| \equiv GW| \equiv \{ID_i, Sn, U_i| \equiv (U_i \overset{M}{\leftrightarrow} S_n), B_i, T'''\}$$

We could get the following statement by applying the BAN logic rule to break conjunctions rule to S_7:

$S_8: S_n|\equiv GW|\equiv U_i|\equiv (U_i \overset{M}{\leftrightarrow} S_n)$.

According to A_{10}, we could get the following statement by applying the jurisdiction rule to S_8:

$S_9: S_n|\equiv U_i|\equiv (U_i \overset{M}{\leftrightarrow} S_n)$

Since $SK = h(ID_i \parallel Sn \parallel M \parallel T'||T^*)$, we could get:

$S_{10}: S_n|\equiv U_i|\equiv (U_i \overset{SK}{\leftrightarrow} S_n)$ (Goal4)

According to A_{11}, we could get the following statement by applying the jurisdiction rule to S_{10}:

$S_{11}: S_n|\equiv (U_i \overset{M}{\leftrightarrow} S_n)$. (Goal3)

According to the message $Msg3$, we could get:

$S_{12}: U_i\{Sn, B_i, M, T*\}_{U_i \overset{SK}{\leftrightarrow} S_n}$

We could get the following statement by applying the message-meaning rule to S_{12}:

$S_{13}: U_i|\equiv S_n|\sim \{Sn, B_i, M, T*\}_{U_i \overset{SK}{\leftrightarrow} S_n}$

According to A_2, we could get the following statement by applying the message-meaning rule to S_{13}:

$S_{14}: U_i|\equiv S_n|\equiv (U_i \overset{SK}{\leftrightarrow} S_n)$. (Goal2)

According to A_{11}, we could get the following statement by applying the jurisdictional rule to S_{14}:

$S_{15}: U_i|\equiv (U_i \overset{SK}{\leftrightarrow} S_n)$. (Goal1)

According to (Goal 1), (Goal 2), (Goal 3) and (Goal 4), we know that both U_i and S_n believe that a session key SK is shared between them.

5.2 Other discussions

In this subsection, we will show that our protocol could satisfy security requirements of the WMSN used in a hospital environment. The details are described as follows:

Mutual authentication In our protocol, only the one with C_{ig} and $h(ID_i||ID_g||K)$ could generate a legal message $m_1 = \{C_{ig}, CID_i, T'\}$, where $N_i^* = h(ID_i||ID_g||K)$, $CID_i = E_{N_i^*}[h(ID_i||C_{ig}||Sn||M||N||T')||Sn||M||N]$ and T' are the current timestamp. Then GW could authenticate U_i by checking the validity of CID_i. Only GW and S_n know the secret key SK_{gs}, then S_n could authenticate GW by checking the validity of $A_i = E_{SK_{gs}}\left[ID_i^{\xi}||Sn^{\xi}||M^{\xi}||B_i||T'''\right]$. At the same time, S_n could authenticate U_i since he trusts the message sent by GW. Only the one with the random number M could generate the session key $SK = h(ID_i||Sn||M||T'||T^*)$ and generate a legal message $m_3 = \{L, T^*\}$, where $L = E_{SK}[Sn||B_i^*||T^*]$ and T^* are the current timestamp. By checking the validity of L, U_i could confirm that m_3 is generated by S_n. Then he could authenticate GW and S_n. Therefore, our protocol could provide mutual authentication among U_i, GW and S_n.

Session key establishment In the execution of our protocol, U_i and S_n could generate a session key by computing $SK = h(ID_i||Sn||M||T'||T^*)$. Therefore, our protocol could generate a session key in its execution. The session key could be used to protect future communications in WMSNs.

Known-key security Suppose an adversary could get a session key $SK = h(ID_i||Sn||M||T'||T^*)$ generated between U_i and S_n. However, he cannot get other session keys generated in other sessions, since new M, T' and T^* are generated in each session key. Therefore, our protocol could provide known-key security.

Low communication and computational cost From the description of our protocol, we know that only bit XOR operation and hash function operation are needed in our protocol. The transmitted message is almost the same as that in Kumar et al.'s protocol. Therefore, we conclude that our protocol inherit the advantages of low communication and computational cost of Kumar et al.'s protocol. Our protocol can provide low communication and computational cost.

User friendliness In our protocol, the health professional U_i could choose his identity ID_i and password PW_i freely. He also could change his password at his will. Therefore, we can conclude that our protocol could provide user friendliness.

User anonymity In our protocol, the health professional's identity ID_i is included in $C_{ig} = E_J[r_g||ID_i||ID_g]$. Without GW's secret key J, the adversary cannot extract ID_i from C_{ig} since $E_{key}[\cdot]$ is a secure symmetric encryption algorithm. Also, the patient's identity is not included in the transmitted message. Therefore, our protocol could provide user anonymity.

Password guessing attack Suppose the adversary could steal U_i's smart card and extract information $\{r_i, C_{ig}, N_i\}$ from the smart card through the side channel attack [20, 21], where $N_i = h(ID_i||ID_g||K) \oplus h(PW_i||r_i)$, $C_{ig} = E_J[r_g||ID_i||ID_g]$ and r_i. He could guess a password PW_i' and compute $N_i' = N_i \oplus h(PW_i'||r_i)$. However, he cannot verify the legality of PW_i'. Therefore, our protocol could withstand the password guessing attack.

Replay attack The adversary may intercept the message transmitted in our protocol and replay it. However, U_i, GW and S_n could find the attack by checking the freshness of $T*$, T' and T''' separately. Therefore, our protocol could withstand the replay attack.

Stolen verifier table attack There is no verifier table is maintained in our protocol. Therefore, the stolen verifier

table attack is not effective for our protocol and our protocol can withstand the attack.

Stolen smart card attack Suppose an adversary could steal U_i's smart card and extract information $\{r_i, C_{ig}, N_i\}$ from the smart card through the side channel attack [20, 21], where $N_i = h(ID_i||ID_g||K) \oplus h(PW_i||r_i)$, $C_{ig} = E_J[r_g||ID_i||ID_g]$ and r_i. He could guess a password PW_i' and compute $N_i' = N_i \oplus h(PW_i'||r_i)$. From the description of our protocol, we know that U_i will replace C_{ig} with a new one after a session. Then the adversary cannot find a message related to N_i and C_{ig}. He cannot verify the legality of PW_i'. Therefore, our protocol can withstand the password guessing attack.

Privileged insider attack In the professional registration phase of our protocol, U_i sends ID_i and $h(PW_i||r_i)$ to GW through a secure channel. The privileged insider cannot get U_i's password since it is protected by the secure hash function and the random number r_i. Therefore, our protocol can withstand the privileged insider attack [23].

Off-line password guessing attack Assume that the adversary A could extract the information stored in a health professional U_i's smart card. He can guess a password. However, he cannot get a message sent by the smart card to verify his guess, since our protocol can provide user anonymity [24, 25].

Man-in-the-middle attack From the above analysis, we know that our protocol could provide mutual authentication among U_i, GW and S_n. Therefore, our protocol could withstand the man-in-the-middle attack.

Impersonation attack To impersonate U_i to GW, the adversary must generate a legal message $m_1 = \{C_{ig}, CID_i, T'\}$, where $CID_i = E_{N_i^*}[h(ID_i||C_{ig}||Sn||M||N||T')||Sn||M||N]$, $N_i^* = h(ID_i||ID_g||K)$ and T' is the current timestamp. It is easy to say that without K, A cannot compute N_i^* and impersonate U_i to GW. To impersonate GW to S_n, A must generate a legal message $m_2 = \{A_i, T'''\}$, where $A_i = E_{SK_{gs}}[ID_i||Sn||M||B_i||T''']$ and T''' is the current timestamp. Without the secret key SK_{gs}, A cannot generate A_i since $E_{key}[\cdot]$ is a secure symmetric encryption algorithm. Therefore, A cannot impersonate GW to S_n. To impersonate S_n to U_i, A must generate a legal message $m_3 = \{L, T^*\}$, where T^* is the current timestamp, $SK = h(ID_i||Sn||M||T'||T^*)$ and $L = E_{SK}[Sn||B_i^*||T^*]$. Without the secret key SK_{gs}, A cannot get M from $A_i = E_{SK_{gs}}[ID_i||Sn||M||B_i||T''']$ and generate m_3. Therefore, A cannot impersonate S_n to U_i. We can conclude that our protocol can withstand the impersonation attack.

6 Functionality and performance analysis

In this section, we will compare the functionality and performance of our protocol with that of three latently published protocols, i.e., Yeh et al.'s [17], Shi and Gong's [19] and Kumar et al.'s protocols [1].

Table 1 Functionality comparisons

	Yeh et al.'s protocol	Shi and Gong's protocol	Kumar et al.'s protocol	Our proposed protocol
E1	No	Yes	Yes	Yes
E2	Yes	Yes	Yes	Yes
E3	Yes	Yes	Yes	Yes
E4	No	No	Yes	Yes
E5	Yes	Yes	Yes	Yes
E6	No	No	No	Yes
E7	No	No	No	Yes

E1 mutual authentication, *E2* session key establishment, *E3* known-key security, *E4* low communication and computational cost, *E5* user friendliness, *E6* user anonymity, *E7* secure against various attacks

The functionality of different protocols is listed in Table 1. As shown in Table 1, our protocol could provide mutual authentication, session key establishment, known-key security, low communication and computational cost, user friendliness and user anonymity. Besides, our protocol could withstand common attacks. Yeh et al.'s [17], Shi and Gong's [19] and Kumar et al.'s protocols [1] could provide less functionality required in health-care applications using WMSNs.

To evaluate the performance of different protocols, we define some notations as follows:

- T_h: The time for executing the hash function operation.
- T_s: The time for executing the symmetric key cryptography operation.
- T_p: The time for executing the elliptic curve point multiplication operation.

Table 2 Performance comparisons

	Yeh et al.'s protocol	Shi and Gong's protocol	Kumar et al.'s protocol	Out protocol
E1	$1\,T_h$	$1\,T_h$	0	$1\,T_h$
E2	$1\,T_h$	$2T_h + T_p$	$1T_h + 1T_s$	$1T_h + 1T_s$
E3	$5T_h + 2T_p$	$5T_h + 3T_p$	$4T_h + 2T_s$	$4T_h + 2T_s$
E4	$2T_h + 3T_p$	$4T_h + 1T_p$	$1T_h + 3T_s$	$2T_h + 5T_s$
E5	$2T_h + 2T_p$	$4T_h + 1T_p$	$1T_h + 2T_s$	$1T_h + 2T_s$
E6	$3T_h$	$4T_h$	$4T_h$	$2T_h$
E7	0	0	0	0

E1 computation cost at the health professional side in the registration phase, *E2* computation cost at the gateway side in the registration phase, *E3* computation cost at the health professional side in the login phase, *E4* computation cost at the gateway side in the login phase, *E5* computation cost at the sensor side in the login phase, *E6* computation cost at the health professional side in the password-changing phase, *E7* computation cost at the gateway side in the password-change phase

Compared with the computational cost of other operation, that of bit XOR operation could be ignored. Then we just counter the hash function operation, the symmetric key cryptography operation and the elliptic curve point multiplication operation in our comparisons. The functionality of different protocols are listed in Table 2. In the registration phase of our protocol, T_h and T_h are needed at the user side and the gateway side separately. Similarly, T_s, T_h and T_s are needed at the user side, the gateway side and the sensor node side separately in the login and authentication phase of our protocol. Besides, T_h is needed at the user side in the password-change phase. Compared with the computational cost of the hash function operation and the symmetric key cryptography operation, that of the elliptic curve point multiplication operation is much more complicated. Besides, the hash function operation and the symmetric key cryptography operation have similar computational cost. Therefore, our protocol and Kumar et al.'s protocol have better performance than Ye et al.'s protocol and Shi and Gong's protocol.

From the above comparisons, our protocol could overcome the weaknesses in Yeh et al.'s [17], Shi and Gong's [19] and Kumar et al.'s protocols [1] and could satisfy the functionality requirements of the WMSN for health-care application. Although Kumar et al.'s protocol [1] has better performance than our protocol, their protocol has three fatal weaknesses. It is acceptable to improve security at the cost of increasing computational cost slightly. Therefore, we can conclude that our protocol is more suitable for health-care applications using WMSNs.

7 Conclusion

With the wide application of WMSNs, protection of privacy and safety in WNSNs becomes more and more urgent. Especially, in health-care applications using WMSNs, attacks may threaten patients' lives. In this paper, we first demonstrate that some security weaknesses in Kumar et al.'s authentication protocol for health-care applications using WMSNs. Then we propose a robust anonymous authentication protocol for health-care applications using WMSNs. Security analysis shows our protocol could overcome the security weaknesses in previous protocols. Performance analysis shows that our protocol has low communication and computational cost. Therefore, our protocol is more suitable for health-care applications using WMSNs.

Acknowledgments The authors thank Prof. Thomas Plagemann and the anonymous reviewers for their valuable comments. This research was supported by the Open Funds of State Key Laboratory of Information Security (No. 2013-3-3) and the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20110141120003).

Conflict of interest The authors declare no conflict of interest.

References

1. Kumar, P., Lee, S., Lee, H.: E-SAP: efficient-Strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors **12**, 1625–1647 (2012)
2. Kumar, P., Lee, Y.D., Lee, H.J.: Secure health monitoring using medical wireless sensor networks. In: Proceedings of the 6th international conference on networked computing and advanced information management (NCM'10), Seoul, Korea, pp. 491–494, 16–18 August 2010
3. Haque, M.M., Pathan, A.S.K., Hong, C.S.: Securing U-healthcare sensor networks using public key based scheme. In Proceeding of the 10th international conference of advance communication technology (ICACT), Seoul, Korea, pp. 1108–1111, 19–22 Febr 2008
4. Dagtas, S., Pekhteryev, G., Sahinoglu, Z., Cam, H., Challa, N.: Real-time and secure wireless health monitoring. Int. J. Telemed. Appl. (2008). doi:10.1155/2008/135808
5. Boukerche, A., Ren, Y.: A secure mobile healthcare system using trust-based multicast scheme. IEEE J. Sel. Areas Commun. **27**, 387–399 (2009)
6. Lin, X., Lu, R., Shen, X., Nemoto, Y., Kato, N.: SAGE: a strong privacy-preserving scheme against global evesdropping for ehealth systems. IEEE J. Sel. Areas Commun. **27**, 365–378 (2009)
7. Malasri, K., Wang, L.: Design and implementation of a secure wireless mote-based medical sensor network. Sensors **9**, 6273–6297 (2009)
8. Hu, F., Jiang, M., Wagner, M., Dong, D.C.: Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/software codesign. IEEE Trans. Inf Technol. Biomed. **11**, 619–627 (2007)
9. Le, X.H., Khalid, M., Sankar, R., Lee, S.: An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. J. Netw. **6**, 355–364 (2011)
10. Huang, Y.M., Hsieh, M.Y., Chao, H.C., Hung, S.H., Park, J.H.: Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. IEEE J. Sel. Areas Commun. **27**, 400–411 (2009)
11. Das, M.L.: Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. **8**, 1086–1090 (2009)
12. Nyang, D., Lee, M.: Improvement of Das's two-factor authentication protocol in wireless sensor networks. Cryptol. ePrint Arch. **2009**, 631 (2009)
13. Huang, H., Chang, Y., Liu, C.: Enhancement of two-factor user authentication in wireless sensor networks. In Proceedings of the 6th international conference on intelligent information hiding and multimedia signal processing (IIHMSP'10). 27–30 (2010)
14. Chen, H., Shih, W.: A robust mutual authentication protocol for wireless sensor networks. ETRI J. **32**, 704–712 (2010)
15. Khan, M.K., Alghathbar, K.: Cryptanalysis and security improvement of 'two-factor user authentication in wireless sensor networks'. Sensors **10**, 2450–2459 (2010)
16. Yoo, S., Park, K., Kim, J.: A security-performance balanced user authentication scheme forwireless sensor networks. Int. J. Distrib, Sens. Netw. (2012) (Article ID 382810)
17. Yeh, H.L., Chen, T.H., Liu, P.C., Kim, T.H., Wei, H.W.: A secure authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors **11**, 4767–4779 (2011)
18. Han, W.: Weakness of a secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Cryptol. ePrint Arch. (2011). http://eprint.iacr.org/2011/293

19. Shi, W., Gong, P.: A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. Int. J. Distrib. Sens. Netw. (2012) (Article ID 730831)
20. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In Proceedings of the advances in cryptology, Santa Barbara, pp. 388–397, 15–19 Aug 1999
21. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smartcard under the threat of power analysis attacks. IEEE Trans. Comput. **51**, 540–552 (2002)
22. He, D., Wu, S., Chen, J.: Note on design of improved password authentication and update scheme based on elliptic curve cryptography. Math. Comput. Model. **55**(3–4), 1661–1664 (2012)
23. He, D., Hu, H.: Cryptanalysis of a dynamic ID-based remote user authentication scheme with access control for multi-server environment. IEICE Trans. Inf. Syst. **E96-D**(1), 138–140 (2013)
24. He, D., Chen, J., Zhang, R.: A more secure authentication scheme for telecare medicine information systems. J. Med. Syst. **36**(3), 1989–1995 (2012)
25. He, D., Chen, Y., Chen, J.: Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn. **69**(3), 1149–1157 (2012)
26. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. ACM Trans. Comput. Syst. **8**, 18–36 (1990)
27. He, D., Wang, D., Wu, S.: Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards. Inf. Technol. Control **42**(2), 170–177 (2013)