Future Generation Computer Systems 80 (2018) 483–495

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A robust and anonymous patient monitoring system using wireless medical sensor networks

Ruhul Amin [a], SK Hafizul Islam [b,*], G.P. Biswas [a], Muhammad Khurram Khan [c], Neeraj Kumar [d]

[a] *Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India*
[b] *Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani 333031, Rajasthan, India*
[c] *Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia*
[d] *Department of Computer Science and Engineering, Thapar University, Patiala 147004, Panjab, India*

HIGHLIGHTS

- A robust and anonymous user authentication protocol is designed to monitor patient health using wireless medical sensor networks.
- The security validation and authentication proof of the proposed protocol is done using AVISPA tool and BAN logic.
- The proposed protocol has superior performance than the existing protocols.

ARTICLE INFO

Article history:
Received 1 September 2015
Received in revised form
23 May 2016
Accepted 25 May 2016
Available online 8 June 2016

Keywords:
Wireless medical sensor network
Password authentication
User anonymity
Hash function
AVISPA tool
BAN logic

ABSTRACT

In wireless medical sensor network (WMSN), bio-sensors are implanted within the patient body to sense the sensitive information of a patient which later on can be transmitted to the remote medical centers for further processing. The patient's data can be accessed using WMSN by medical professionals from anywhere across the globe with the help of Internet. As the patient sensitive information is transmitted over an insecure WMSN, so providing a secure access and privacy of the patient's data are challenging issues in WMSN environments. However, in literature, to provide secure data access, few user authentication protocols exist. Most of these existing protocols may not be applicable to WMSNs for providing user's anonymity. To fill these gaps, in this article, we propose an architecture for patient monitoring health-care system in WMSN and then design an anonymity-preserving mutual authentication protocol for mobile users. We used the AVISPA tool to simulate the proposed protocol. The results obtained indicate that the proposed authentication protocol resists the existing well known attacks. In addition, the BAN logic model confirms mutual authentication feature of the proposed protocol. Moreover, an informal cryptanalysis is also given, which ensures that the proposed protocol withstands all known attacks. We perform a comparative discussion of the proposed protocol against the existing protocols and the comparative results demonstrate that the proposed protocol is efficient and robust. Specifically, the proposed protocol is not only effective in providing robustness against common security threats, but it also offers an efficient login, robust mutual authentication, and user-friendly password change.

1. Introduction

With the advancement of wireless communication and mobile technologies, health-care industry utilizes these technologies in patient monitoring system, where the medical professional can monitor patient's health from anywhere and anytime. The medical professional monitors various health conditions of a patient through wireless communication using the mobile and the sensor devices. The sensor devices sense the health information of the patient, and send it to the medical professional via a gateway node of the WMSN. Since the sensitive patient information is transmitted through an open channel, so there is a big concern of message security against various types of active and passive attacks. To make secure communication between medical

* Corresponding author.
E-mail addresses: amin_ruhul@live.com (R. Amin), hafi786@gmail.com (S.H. Islam), gpbiswas@gmail.com (G.P. Biswas), mkhurram@ksu.edu.sa (M.K. Khan), neeraj.kumar@thapar.edu (N. Kumar).

http://dx.doi.org/10.1016/j.future.2016.05.032
0167-739X/

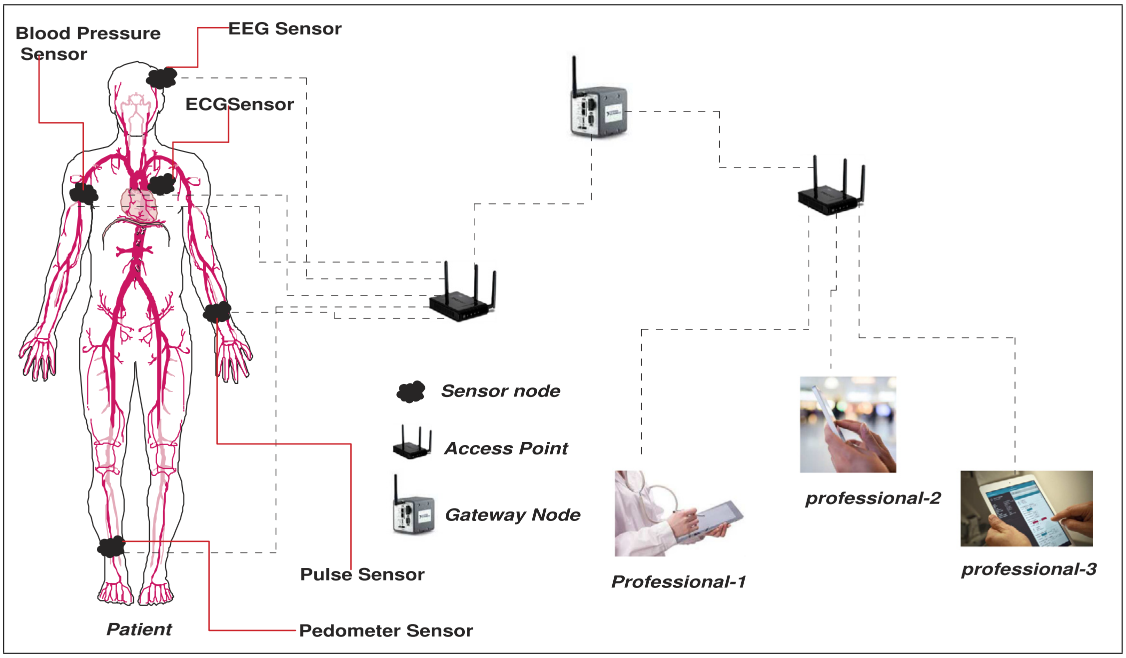

Fig. 1. The proposed patient monitoring architecture using WMSN.

professional and patient, user authentication with session key agreement protocols [1–5] are widely used. In such protocols, after sharing a common session key between the medical professional and the patient, information can easily be transmitted through open channel by encrypting the message with the session key. In such protocols, session key verification [6] is one of the important security aspects to get assurance about the establishment of the common and secret session key between different participants.

In the literature, lots of user authentication and session key agreement protocols are designed using RSA cryptosystem [7], ECC system [8,9], bilinear pairing [10], chaotic map [11], and hash function [12–19]. As mentioned in [6], the ECC cryptosystem is more secure and efficient than the RSA system. In cryptography, the bilinear pairing is the most expensive operation than other operations and hence, it is not appropriate for resource-constrained WMSN. On the other hand, the chaotic map is also more expensive compared with the hash function. It is known that hash function is most lightweight function and popularly used to design various cryptographic protocols for resource-constrained environments. In WMSN, sensor nodes are generally powered by small batteries and recharging of the nodes is problematic. In addition, mobile devices, such as PDAs and smartphones are not suitable to compute expensive operations due to low computing processor.

1.1. Architecture of patient monitoring system using WMSN

Sensor node is a transducer, which senses various characteristics from different environments and then forwards the sensed data to the base stations located across different geographical locations. Nowadays, the sensor networks are used widely in numerous applications, such as health-care monitoring, environmental monitoring, water quality monitoring and forest fire detection. In this article, we consider the health-care monitoring system as shown in Fig. 1. We have provided a model for patient monitoring system usable in sensor networks. The proposed model consists of the participants, such as medical professional (doctor, patient, nurse, pathologist, etc.), sensors and gateway nodes. The sensor nodes sense the physical condition of the patient and then sends the data to the gateway node through an access point. The gateway node is the heart of the proposed model and is used to provide registration to all the medical professionals. The medical professionals gather the sensitive information of the patient from the gateway node to analyze the data and monitor the patient's physical conditions.

As mentioned in [20], the communication cost of the sensor node depends on transmitting and receiving l-bits messages and also it is directly proportional to the distance between the sensor node and the target entity. Therefore, the distance should be minimized between them. In the protocols proposed in [21–23], we have found that the sensor nodes directly transmit sensed information to the medical professional. Therefore, in these protocols, the communication cost for the sensor nodes is high and the lifetime of the nodes gradually decreases and reaches to the dead state. In order to avoid this difficulty, we proposed a modified architecture in Fig. 1, where the sensed information reaches to the medical professional via the gateway nodes.

1.2. Discussions on the related works

In order to provide secure health-care monitoring of the patient over WMSN, we observed that very less number of efficient and robust authenticated and key agreement protocols [20–25] have been put forward in the existing literature. In 2012, Kumar et al. [21] suggested an authentication protocol for WMSN to monitor the health conditions of a patient and stated that the protocol can defend against known security threats. But, the works proposed in [22,24] elucidates that the protocol [21] is weak against some security threats. In addition, they proposed an enhanced protocol to achieve more efficiency and robustness against known attacks. In 2015, Li et al. [25] and Wu et al. [23] showed that the scheme put forwards by He et al. [22] suffers from off-line password guessing and impersonation attacks. Li et al. further demonstrated the protocol in [22] is unable to detect the wrong inputs, which are entered by mistake during the login phase and password change phase. Li et al. [25] and Wu et al. [23] both independently proposed two improved user authentication protocols using smartcard and hash function to remove the loopholes of the protocol in [22].

1.3. Motivation and contributions

The WMSN provides a platform to monitor health condition of the patient from remote location over insecure networks. In the existing authentication protocols, the researchers have considered user anonymity, user untraceability, mutual authentication, attack resilience against different attacks, and energy consumption of the sensor nodes as the key factors for the authentication protocols suitable for the applications of health-care technologies. Therefore, many research articles suggested different solutions, but still none of the solutions are sufficient to provide known security features as discussed in Sections 1.1 and 1.2. Therefore, we have been motivated to design a more robust and user-friendly patient monitoring system in WMSN. The following contributions have been achieved in this article:

(1) We have presented a health monitoring system architecture used for WMSN (see Fig. 1), which reduces the energy consumption of the sensor nodes.
(2) We have proposed hash function-based mutual authentication and session key negotiation protocol, which provides user anonymity for medical professional.
(3) We have used AVISPA tool [26–28] to measure security strength of our protocol. The results obtained showed that the proposed protocol is SAFE in the OFMC and CL-AtSe models against the active and passive attacks.
(4) We have verified the mutual authentication property of the proposed protocol using BAN logic model [29].
(5) We have performed a comparative discussion of the proposed protocol with various existing protocols and the comparison results demonstrated that the proposed protocol is more robust and secure than the other existing protocols of its category.

1.4. Construction of the article

The proposed protocol is described in Section 2. The simulation results including brief idea of AVISPA software are given in Section 3. The BAN logic model ensures the mutual authentication correctness of the proposed protocol and presents in Section 4. Section 5 demonstrated that the proposed protocol defeats various known security attacks. Section 6 presents performance comparison results of the proposed protocol with other existing protocols. Finally, the article is concluded with future insights in Section 7.

2. Proposed protocol

In Section 1.1, we discussed the proposed model for WMSN. We then present the proposed authentication and key negotiation protocol to make secure data transmission. The proposed authentication protocol includes five phases namely (1) Setup, (2) Medical professional registration, (3) Patient registration, (4) Login and authentication, and (5) Password change phase. All the notations are represented in Table 1.

2.1. Setup phase

The registration center first chooses a long-term secret key K for the GW and then computes a secret key $SK_{GW-SN_j} = h(ID_{SN_j} \parallel K)$ for SN_j, where $1 \leq j \leq n$ and n represents the number of sensor nodes. The proposed protocol uses the light-weight cryptographic general hash function and it is defined as $h : \{0, 1\}^* \rightarrow \{0, 1\}^l$, where l is the output length of $h(\cdot)$.

Table 1
Notations employed in the proposed protocol.

Symbol	Description
U_i	Medical professional
GW	Gateway node
SN_j	Sensor node
PW_i	Password of U_i
ID_i	Identity of U_i
ID_{SN_j}	Identity of SN_j
K	Secret key of GW
TID_i	Unique temporary identity generated by GW for U_i
R_1	Random nonce created by U_i
R_2	Random nonce created by GW
R_3	Random nonce created by SN_j
$h(\cdot)$	Cryptographic one-way hash function
$\parallel$	Concatenation operation
$\oplus$	Bitwise XOR operation

2.2. Medical professional registration phase

In order to provide health-care services, a medical professional U_i must execute this phase. In this phase, U_i and GW perform all the steps stated below:

Step 1: U_i picks an identity ID_i, password PW_i, and then calculates $HPW_i = h(ID_i \oplus PW_i)$. Then, he/she sends $\langle ID_i, HPW_i \rangle$ to GW securely either using the TLS protocol or in off-line mode [20,25].

Step 2: After receiving $\langle ID_i, HPW_i \rangle$, GW computes $Reg_i = h(ID_i \parallel R_i \parallel HPW_i)$, $A_i = R_i \oplus HPW_i$, $B_i = h(ID_i \parallel R_i \parallel K)$, $C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i)$, $D_i = R_i \oplus h(TID_i \parallel K)$, where R_i and TID_i are the random number and temporary identity of U_i. In order to avoid the untraceability attack, GW selects different TID_i in each session.

Step 3: GW stores $\langle TID_i, D_i \rangle$ in a table for further use and forwards $\langle TID_i, Reg_i, A_i, C_i, h(\cdot) \rangle$ to U_i through a secure communication channel. After receiving $\langle TID_i, Reg_i, A_i, C_i, h(\cdot) \rangle$, U_i stores all these information into his/her mobile device.

We further present the medical professional registration phase in Fig. 2.

2.3. Patient registration phase

This phase is analogous to the patient registration phase proposed in Wu et al.'s protocol [23]. At first, the patient selects and forwards his/her name to the registration center and then it selects an appropriate sensor kit and appoints medical professional. Finally, the registration center forwards patient's identity and relevant data about medical sensor to the corresponding medical professional.

2.4. Login and authentication phase

The execution of this phase achieve mutual authentication and session key negotiation between the participants involved in the protocol. The description of this phase is expressed below.

Step 1: U_i inputs ID_i and PW_i into the mobile device. Then, it calculates $HPW_i^* = h(ID_i \oplus PW_i)$, $R_i^* = A_i \oplus HPW_i$, $Reg_i^* = h(ID_i \parallel R_i^* \parallel HPW_i^*)$, and verifies whether $Reg_i^* ?= Reg_i$ holds. If it is not valid, the mobile device aborts the login request, otherwise, proceeds for further operations.

Step 2: The mobile device produces a random nonce R_1 and calculates $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \parallel HPW_i^*)$, $CID_i = ID_i \oplus h(TID_i \parallel R_i^* \parallel T_1)$, $M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1)$, $M_2 = h(R_i \parallel T_1) \oplus R_1$ and then sends $\langle TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 \rangle$ to GW through an insecure channel.

U_i/**Mobile device**		GW
Choose ID_i, PW_i		
Compute $HPW_i = h(ID_i \oplus PW_i)$		
	$\xrightarrow{\langle ID_i, HPW_i \rangle}$ (via a secure channel)	
		Generate R_i
		Compute $Reg_i = h(ID_i \parallel R_i \parallel HPW_i)$
		Compute $A_i = R_i \oplus HPW_i$
		Compute $B_i = h(ID_i \parallel R_i \parallel K)$
		Compute $C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i)$
		Compute $D_i = R_i \oplus h(TID_i \parallel K)$
		Store $\langle TID_i, D_i \rangle$ in a table
	$\xleftarrow{\langle (TID_i, Reg_i, A_i, C_i, h(\cdot)) \rangle}$ (via a secure channel)	
Store $\langle TID_i, Reg_i, A_i, C_i, h(\cdot) \rangle$ in the mobile device		

Fig. 2. Medical professional registration phase.

Step 3: GW searches the table against TID_i, retrieves D_i and calculates $R_i^* = D_i \oplus h(TID_i \parallel K)$, $ID_i^* = CID_i \oplus h(TID_i \parallel R_i^* \parallel T_1)$, $B_i^* = h(ID_i^* \parallel R_i^* \parallel K)$, $R_1^* = M_2 \oplus h(R_i^* \parallel T_1)$, $M_1^* = h(ID_i^* \parallel B_i^* \parallel R_1^* \parallel T_1)$. GW now checks whether $M_1^* ? = M_1$ holds. If this condition is correct, GW assumes that the message sent by U_i is authentic; otherwise, discontinues the protocol's operations.

Step 4: After verifying the legitimacy of U_i, GW produces a random number R_2 and then calculates $SK_{GW-SN_j} = h(ID_{SN_j} \parallel K)$, $M_3 = h(h(h(ID_i \parallel R_1^* \parallel R_2) \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2)$, $M_4 = h(ID_i \parallel R_1 \parallel R_2) \oplus SK_{GW-SN_j}$, $M_5 = R_2 \oplus h(SK_{GW-SN_j})$. Finally, GW forwards $\langle M_3, M_4, M_5 \rangle$ to SN_j through an insecure network.

Step 5: SN_j calculates $R_2' = M_5 \oplus h(SK_{GW-SN_j})$, $M_6' = M_4 \oplus SK_{GW-SN_j}$, $M_3' = h(h(M_6' \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2')$ and then checks whether $M_3' ? = M_3$ holds. If it is true, SN_j generates a random number R_3 and computes $SK = h(M_6' \parallel R_2 \parallel R_3)$, $M_7 = h(SK \parallel R_3 \parallel SK_{GW-SN_j})$, $M_8 = h(R_2) \oplus R_3$. Finally, SN_j sends $\langle M_7, M_8 \rangle$ to GW through an insecure network.

Step 6: After receiving $\langle M_7, M_8 \rangle$, GW computes $R_3' = M_8 \oplus h(R_2)$, $SK' = h(h(ID_i \parallel R_1 \parallel R_2) \parallel R_2 \parallel R_3')$, $M_7' = h(SK' \parallel R_3' \parallel SK_{GW-SN_j})$, and then checks whether $M_7' ? = M_7$ holds. If it is incorrect, GW aborts the connection, otherwise, generates a new unique identity $TID_i' (\neq TID_i)$ and then computes $M_9 = R_2 \oplus h(ID_i \parallel R_1)$, $M_{10} = h(ID_i \parallel SK' \parallel R_3')$, $M_{11} = TID_i' \oplus h(R_2 \oplus R_3)$. Finally, GW sends $\langle M_8, M_9, M_{10}, M_{11} \rangle$ to U_i through an insecure network.

Step 7: After receiving $\langle M_8, M_9, M_{10}, M_{11} \rangle$, U_i computes $R_2^* = M_9 \oplus h(ID_i \parallel R_1)$, $R_3^* = M_8 \oplus h(R_2^*)$, $TID_i' = M_{11} \oplus h(R_2^* \oplus R_3^*)$, $SK^* = h(h(ID_i \parallel R_1 \parallel R_2^*) \parallel R_2^* \parallel R_3^*)$, $M_{10}^* = h(ID_i \parallel SK^* \parallel R_3^*)$, and then checks whether $M_{10}^* ? = M_{10}$ holds. If it is correct, U_i believes that $\langle M_8, M_9, M_{10}, M_{11} \rangle$ is valid and then sends a confirmation message to GW. The mobile device now updates old TID_i with the new TID_i'. Similarly, GW computes new value $D_i' = R_i \oplus h(TID_i' \parallel K)$ and replaces $\langle TID_i, D_i \rangle$ with $\langle TID_i', D_i' \rangle$.

We further provide the explanation of this phase in Fig. 3.

2.5. Password change phase

This phase periodically updates the old password to a new password. This phase is explained as follows:

Step 1: U_i inputs ID_i and PW_i into the mobile device. Then, it performs $HPW_i^* = h(ID_i \oplus PW_i)$, $R_i^* = A_i \oplus HPW_i$, $Reg_i^* = h(ID_i \parallel R_i^* \parallel HPW_i^*)$ and checks whether $Reg_i^* ? = Reg_i$ is correct. If it is false, the mobile device aborts the password change phase, otherwise, proceeds for further computations.

Step 2: After verifying the legitimacy of U_i, the mobile device requests U_i to enter new password.

Step 3: U_i inputs a new password PW_i^{new}, then the mobile device calculates $HPW_i^{new} = h(ID_i \oplus PW_i^{new})$, $Reg_i^{new} = h(ID_i \parallel R_i^* \parallel HPW_i^{new})$, $A_i^{new} = R_i^* \oplus HPW_i^{new}$, $B_i = h(ID_i \parallel R_i \parallel K)$, $C_i^{new} = B_i \oplus h(ID_i \oplus R_i^* \oplus HPW_i^{new})$. Finally, the mobile device drops $\langle Reg_i, A_i, C_i \rangle$ and stores $\langle Reg_i^{new}, A_i^{new}, C_i^{new} \rangle$ into the mobile device. Thus, U_i can easily change the password without involvement of GW.

We further provide the explanation of this phase in Fig. 4.

3. Simulation of the proposed protocol using AVISPA tool

This section provides the explanation about the simulation procedure of the proposed protocol using the AVISPA tool [20,27,28]. First, we briefly discuss the concept of AVISPA software. Then, we present the HLPSL code of all the participants involved in the proposed protocol and then present the simulation results.

3.1. Brief description of AVISPA tool

The *AVISPA* is a well known simulation tool, which is used to simulate the security protocol to check whether the security protocol is secure against active and passive attacks. It supports High Level Protocol Specification Language (*HLPSL*). It is to be noted that *AVISPA* [26] also supports four different back-ends and abstraction based methods, which are integrated through *HLPSL*. The description of all these four back-ends can be found in [20,27,28].

3.2. Specification of the proposed protocol

This part concisely presents the role of each participant of the proposed protocol, namely the medical professional U_i, the gateway node GW, the sensor node SN_j, the session, the goal and the environment. In Fig. 5, the role of U_i in *HLPSL* is implemented. During the execution of the medical professional registration phase, U_i sends the registration message *Snd*({*IDi.HPWi*'}_*SKj*) to GW through secure channel using the symmetric key SK_j and *Snd*() operation. The type declaration *channel*(*dy*) tells that the channel follows Dolev and Yao threat model [30].

U_i/**Mobile device**	GW	SN_j
Input $\langle ID_i, PW_i\rangle$ Compute $HPW_i^* = h(ID_i \oplus PW_i)$ Compute $R_i^* = A_i \oplus HPW_i$ Compute $Reg_i^* = h(ID_i \parallel R_i^* \parallel HPW_i^*)$ If $(Reg_i^* \neq Reg_i)$, abort the connection Else, generate R_1 Compute $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \parallel HPW_i^*)$ Compute $CID_i = ID_i \oplus h(TID_i \parallel R_i^* \parallel T_1)$ Compute $M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1)$ Compute $M_2 = h(R_i \parallel T_1) \oplus R_1$ $\xrightarrow{\langle TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1\rangle}$ (via an insecure channel)		
	Retrieve ID_i from the table Compute $R_i^* = D_i \oplus h(TID_i \parallel K)$ Compute $ID_i^* = CID_i \oplus h(TID_i \parallel R_i^* \parallel T_1)$ Compute $B_i^* = h(ID_i^* \parallel R_i^* \parallel K)$ Compute $R_1^* = M_2 \oplus h(R_i^* \parallel T_1)$ Compute $M_1^* = h(ID_i^* \parallel B_i^* \parallel R_1^* \parallel T_1)$ If $(M_1^* \neq M_1)$, abort the connection Else, compute $SK_{GW-SN_j} = h(ID_{SN_j} \parallel K)$ Compute $M_3 = h(h(h(ID_i \parallel R_1^* \parallel R_2) \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2)$ Compute $M_4 = h(ID_i \parallel R_1 \parallel R_2) \oplus SK_{GW-SN_j}$ Compute $M_5 = R_2 \oplus h(SK_{GW-SN_j})$ $\xrightarrow{\langle M_3, M_4, M_5\rangle}$ (via an insecure channel)	
		Compute $R_2' = M_5 \oplus h(SK_{GW-SN_j})$ Compute $M_6' = M_4 \oplus SK_{GW-SN_j}$ Compute $M_3' = h(h(M_6' \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2')$ If $(M_3' \neq M_3)$, reject Else, generate R_3 Compute $SK = h(M_6' \parallel R_2 \parallel R_3)$ Compute $M_7 = h(SK \parallel R_3 \parallel SK_{GW-SN_j})$ Compute $M_8 = h(R_2) \oplus R_3$ $\xleftarrow{\langle M_7, M_8\rangle}$ (via a insecure channel)
	Compute $R_3' = M_8 \oplus h(R_2)$ Compute $SK' = h(h(ID_i \parallel R_1 \parallel R_2) \parallel R_2 \parallel R_3')$ Compute $M_7' = h(SK' \parallel R_3' \parallel SK_{GW-SN_j})$ If $(M_7' \neq M_7)$, abort the connection Else, generate unique $TID_i'(\neq TID_i)$ Compute $M_9 = R_2 \oplus h(ID_i \parallel R_1)$ Compute $M_{10} = h(ID_i \parallel SK' \parallel R_3')$ Compute $M_{11} = TID_i' \oplus h(R_2 \oplus R_3)$ $\xleftarrow{\langle M_8, M_9, M_{10}, M_{11}\rangle}$ (via a insecure channel)	
Compute $R_2^* = M_9 \oplus h(ID_i \parallel R_1)$ Compute $R_3^* = M_8 \oplus h(R_2^*)$ Compute $TID_i' = M_{11} \oplus h(R_2^* \oplus R_3^*)$ Compute $SK^* = h(h(ID_i \parallel R_1 \parallel R_2^*) \parallel R_2^* \parallel R_3^*)$ Compute $M_{10} = h(ID_i \parallel SK^* \parallel R_3^*)$ If $(M_{10}^* \neq M_{10})$, abort the connection Else, update TID_i by TID_i' $\xrightarrow{\langle \text{confirmation message}\rangle}$		
	Compute $D_i' = R_i \oplus h(TID_i' \parallel K)$ Replace $\langle TID_i, D_i\rangle$ with $\langle TID_i', D_i'\rangle$	

Fig. 3. Login and authentication phases.

The declaration $secret(PWi, scrt0, Ui)$ and $secret(IDi, scrt1, \{Ui, GW\})$ denote that PW_i and ID_i are known to Ui and GW, respectively. In transition 2, U_i receives information $Rcv(TIDi', Regi', Ai', Ci')$ from GW securely for the mobile device using the $Rcv()$ operation. After that, U_i creates $R1'$ and timestamp $T1'$ using $new()$ operation. Then U_i sends $\{TIDi, IDSNj, CIDi', M1', M2', T1'\}$ to GW through insecure networks. The statement $witness(Ui, GW, alice\_bob, R1')$ means that U_i has newly created the value $R1'$ for GW and the declaration $secret(\{R1', Ri\}, scrt3, \{Ui, GW\})$ tells that $R1', Ri$ are only known to U_i and GW. In transition 3, U_i receives $Rcv(M8', M9', M10', M11')$ through a public channel and calculates the key of the protocol. The declaration $secret(SK', scrt4, \{Ui, GW, SNj\})$ represents that the session key negotiation between all the participants are secure.

We presented the role for GW in *HLPSL* language in Fig. 6. At first, GW receives the registration message $Rcv(\{IDi.HPWi'\}\_SKj)$ securely from U_i using SKj and then GW generates unique temporary identity $TIDi$ and random number Ri. Then, GW sends $Snd(TIDi', Regi', Ai', Ci')$ securely to U_i. In transition 2, GW receives $Rcv(TIDi, IDSNj, CIDi', M1', M2', T1')$ from U_i as login message and then generates the random number $R2$ using $new()$ operation. Then, GW forwards $Snd(M3', M4', M5')$ to S_j. The declaration $witness(GW, SNj, bob\_sensor, R2')$ states that GW has freshly generated $R2$ for SN_j. Moreover, the declaration $secret(SKGSN, scrt5, \{GW, SNj\})$ indicates that $SKGSN$ is shared between GW and SN_j. In transition 3, GW receives $Rcv(M7', M8')$ through an open channel from SN_j and then calculates the session

U_i		Mobile device
Input $\langle ID_i, PW_i \rangle$		
	$\xrightarrow{\langle ID_i, PW_i \rangle}$	
		Compute $HPW_i^* = h(ID_i \oplus PW_i)$ Compute $R_i^* = A_i \oplus HPW_i$ Compute $Reg_i^* = h(ID_i \parallel R_i^* \parallel HPW_i^*)$ If $(Reg_i^* \neq Reg_i)$, abort this operation Else, ask U_i for a new password
	$\xleftarrow{\langle \text{Enter a new password} \rangle}$	
Input s new password PW_i^{new}		
	$\xrightarrow{\langle PW_i^{new} \rangle}$	
		Compute $HPW_i^{new} = h(ID_i \oplus PW_i^{new})$ Compute $Reg_i^{new} = h(ID_i \parallel R_i^* \parallel HPW_i^{new})$ Compute $A_i^{new} = R_i^* \oplus HPW_i^{new}$ Compute $B_i = h(ID_i \parallel R_i \parallel K)$ Compute $C_i^{new} = B_i \oplus h(ID_i \oplus R_i^* \oplus HPW_i^{new})$ Replace $\langle Reg_i, A_i, C_i \rangle$ by $\langle Reg_i^{new}, A_i^{new}, C_i^{new} \rangle$

Fig. 4. Password change phase.

```
role alice (Ui, GW, SNj : agent,
H : hash_func,
SKj : symmetric_key,
Snd, Rcv : channel(dy))
played_by Ui
def=
local State : nat,
IDi,PWi,HPWi,Ri,R1,R2,R3, Regi, Ci, K, T1,
 Ai, Bi, CIDi, M1, M2, M8, IDSNj, TIDi, TIDii,
 M9, M10, M11, SK: text
const alice_bob, bob_sensor, sensor_bob,
scrt0, scrt1, scrt2, scrt3, scrt4: protocol_id
init State := 0
transition
1. State = 0 /\ Rcv(start)=|>
State' := 1 /\ HPWi' := H(xor(IDi,PWi))
/\ secret({PWi}, scrt0, {Ui})
/\ secret({IDi}, scrt1, {Ui,GW})
/\ Snd({IDi. HPWi'}_SKj)
2. State = 1 /\ Rcv(TIDi',Regi',Ai',Ci')=|>
State':=2 /\ R1' := new()
/\ T1' := new()
/\ Ri' := xor(Ai,HPWi)
/\ Bi' := xor(Ci, H(xor(IDi,Ri',HPWi)))
/\ CIDi' := xor(IDi, H(TIDi.Ri'.T1'))
/\ M1' := H(IDi.Bi'.R1'.T1')
/\ M2' := xor(H(Ri'.T1'),R1')
/\ Snd(TIDi,IDSNj,CIDi',M1',M2',T1')
/\ secret({R1', Ri}, scrt2, {Ui,GW})
/\ witness(Ui, GW, alice_bob, R1')
3. State = 2 /\ Rcv(M8', M9', M10', M11') =|>
State' := 3 /\ R2' := xor(M9, H(IDi.R1))
/\ R3' := xor(M8, H(R2'))
/\ TIDii' := xor(M11, H(xor(R2'.R3')))
/\ SK' := H(H(IDi.R1.R2').R2'.R3')
/\secret({SK'}, scrt3, {Ui,GW,SNj})
end role
```

Fig. 5. HLPSL specification of the medical professional U_i of the proposed protocol.

```
role bob ( Ui, GW, SNj : agent,
H : hash_func,
SKj : symmetric_key,
Snd, Rcv : channel(dy))
played_by GW
def=
local State : nat,
IDi,PWi,HPWi,Ri,R1,R2,R3, Regi, Ci, K, Di, T1, Ai,
Bi, CIDi, M1, M2, IDSNj, TIDi, TIDii, M9, M10,
M11, SK, SKGSN, M3, M4, M5, M7, M8: text
const alice_bob, bob_sensor, sensor_bob, scrt0, scrt1,
scrt2, scrt3, scrt4 : protocol_id
init State := 0
transition
1. State = 0 /\ Rcv({IDi. HPWi'}_SKj)=|>
State' := 1 /\ Ri' :=new()
/\ TIDi' := new()
/\ Regi' := H(IDi.Ri'.HPWi)
/\ Ai' := xor(Ri', HPWi)
/\ Bi' := H(IDi.Ri'.K)
/\ Ci' := xor(Bi', H(xor(IDi,Ri',HPWi)))
/\ Di' := xor(Ri', H(TIDi'.K))
/\ Snd(TIDi',Regi',Ai',Ci')
2. State = 1 /\ Rcv(TIDi,IDSNj,CIDi',M1',M2',T1') =|>
State' := 2 /\ R2' := new()
/\Ri' := xor(Di, H(TIDi.K))
/\ R1' := xor(M2,H(Ri',T1))
/\ SKGSN' := H(IDSNj.K)
/\ M3' := H(H(H(IDi.R1'.R2').1).SKGSN'.R2')
/\ M4' := xor(H(IDi.R1'.R2'), SKGSN)
/\ M5' := xor(R2',H(SKGSN))
/\Snd(M3', M4', M5')
/\witness(GW, SNj, bob_sensor, R2')
/\ secret({SKGSN}, scrt4, {GW,SNj})
/\request(Ui, GW, alice_bob, R1)
3. State = 2 /\ Rcv(M7', M8') =|>
State' := 3 /\ R3' := xor(M8, H(R2))
/\ SK' := H(H(IDi.R1.R2).R2.R3')
/\ TIDii' := new()
/\ M9' := xor(R2, H(IDi.R1))
/\ M10' := H(IDi.SK'.R3')
/\ M11' := xor(TIDii', H(xor(R2,R3')))
/\ Snd(M8', M9', M10', M11')
/\ request(SNj, GW, sensor_bob, R3)
end role
```

Fig. 6. HLPSL specification of the gateway node *GW* of the proposed protocol.

key of the protocol. Finally, GW sends $Snd(M8', M9', M10', M11')$ to U_i through a insecure channel using $Snd()$ operation.

In Fig. 7, we present sensor node's S_j role in *HLPSL*, where SN_j first receives $Rcv(M3', M4', M5')$ from GW. Then, SN_j creates a random number $R3$ and computes the session key of the protocol. The declaration $witness(SNj, GW, sensor\_bob, R3')$ tells that SN_j has generated freshly the random number $R3$ for GW. Finally, SNj sends $Snd(M7', M8')$ to GW through an open channel.

In Fig. 8, the role of session, goal and environment have presented in *HLPSL*. All the basic roles and also roles for U_i, GW and SN_j are instanced with concrete arguments in the session segment. Global constant and composition as well as intruder knowledge are given in environment section. The proposed protocol uses the current version (2006/02/2013), which supports secrecy goals and authentication objectives. However, the proposed protocol uses five secrecy goals and three authentications objectives in simulation operation.

3.3. Goals and authentication objectives

- **G0**. $secrecy\_of\, scrt0$ represents that PW_i is only known to U_i.

```
role sensor ( Ui, GW, SNj : agent,
H : hash_func,
SKj : symmetric_key,
Snd, Rcv : channel(dy))
played_by SNj
def=
local State : nat,
IDi,R1,R2,R3, K, IDSNj, SK, SKGSN,
M3, M4, M5, M6, M7, M8: text
const alice_bob, bob_sensor, sensor_bob,
scrt0, scrt1, scrt2, scrt3, scrt4 : protocol_id
init State := 0
transition
1. State=0/\ Rcv(M3', M4', M5') =|>
State':=1 /\ R3' := new()
/\ M6' := xor(M4,SKGSN)
/\ R2' := xor(M5, H(SKGSN))
/\ SK' := H(M6'.R2'.R3')
/\ M7' := H(SK'.R3'.SKGSN)
/\ M8' := xor(H(R2'),R3)
/\ witness(SNj, GW, sensor_bob, R3')
/\ request(GW, SNj, bob_sensor, R2)
/\ Snd(M7', M8')
end role
```

Fig. 7. HLPSL specification of the sensor node SN_j of the proposed protocol.

```
role session(Ui, GW, SNj: agent,
H : hash_func,
SKj : symmetric_key)
def=
local S1, S2, S3, P1, P2, P3: channel (dy)
composition
alice(Ui, GW, SNj, H, SKj, S1, P1)
/\ bob (Ui, GW, SNj, H, SKj, S2, P2)
/\ sensor(Ui, GW, SNj, H, SKj, S3, P3)
end role
role environment()
def=
const ui, gw, snj: agent,
h: hash_func,
skj: symmetric_key,
idi,pwi,regi, hpwi,ai,bi,ci,k,ri,r1,r2,r3,m1,m2,
m3,m4,m5,m6,m7,m8,m9,m10,m11,
skgsn,idsnj,tidi,tidii,di,sk: text,
alice_bob, bob_sensor, sensor_bob, scrt0,
scrt1, scrt2, scrt3, scrt4 : protocol_id
intruder_knowledge = {ui, gw, snj, h, regi, ci,
ai, tidi, m3, m4, m5, m7, m8, m9, m10, m11}
composition
session(ui, gw, snj, h, skj)
/\ session(ui, gw, snj, h, skj)
/\ session(ui, gw, snj, h, skj)
end role
goal
secrecy_of scrt0
secrecy_of scrt1
secrecy_of scrt2
secrecy_of scrt3
secrecy_of scrt4
authentication_on alice_bob_R1
authentication_on bob_sensor_R2
authentication_on sensor_bob_R3
end goal
environment()
```

Fig. 8. HLPSL specification of the session of the proposed protocol.

- **G1**. *secrecy_of scrt*1 represents ID_i is kept secret by U_i and GW.
- **G2**. *secrecy_of scrt*2 represents that the random numbers $R1$, $R2$ used in the proposed protocol are kept secret by U_i and GW.
- **G3**. *secrecy_of scrt*3 signifies that the negotiated secret key of the proposed protocol is only known to U_i, GW and SN_j.

```
% OFMC
% Version of 2006/02/13

SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
/home/avispa/web-interface-computation/./
tempdir/workfilesasld22dXn.if

GOAL
as_specified

BACKEND
OFMC

COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 1.09s
visitedNodes: 64 nodes
depth: 4 plies
```

Fig. 9. Simulated result of the proposed protocol in OFMC back-end.

- **G4**. *secrecy_of scrt*4 signifies that the secret key *SKGSN* used in the proposed protocol is shared between GW and SN_j.
- **A1**. *authentication_on alice_bob_R*1 signifies that U_i creates a random number $R1$ and if GW obtains it securely via message, GW then corroborates U_i.
- **A2**. *authentication_on bob_sensor_R*2 signifies that GW creates a random number $R2$ and if SN_j obtains it securely via message, SN_j then corroborates GW.
- **A3**. *authentication_on sensor_bob_R*3 signifies that SN_j creates a random number $R3$ and if GW obtains it securely via message, GW then corroborates SN_j.

3.4. Simulation results

This section discusses the simulation report obtained after executing the *HLPSL* code into the *AVISPA* software. We found the protocol is "SAFE" under *OFMC* and *CL-AtSe* as simulation results, which are incorporated in Figs. 9 and 10, respectively. The results obtained using tool ensure the strong security on passive and active threats.

4. Authentication correctness using BAN logic model

The BAN includes a set of rules to verify the message source, freshness and origin's trustworthiness of the authentication protocol. In other words, it helps to analyze whether the exchanged messages is trustworthy, secured against eavesdropping, or both. Therefore, we used the BAN logic model to validated the proposed protocol. The description of the BAN logic model can be found in [10,20,29]. We describe below some preliminaries of the BAN logic model for better understanding.

- **Principals** are the agents involved in the protocol (usually people or programs).
- **Keys** are used to encrypt messages symmetrically.
- **Public Keys** are similar to **Keys** except that they are used in pairs.
- **Nonces** are message parts that are not meant to be repeated.
- **Timestamps** are similar to **Nonces** in that they are unlikely to be repeated.

```
SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL

PROTOCOL
/home/avispa/web-interface-computation/./
tempdir/workfile95yQmezGJW.if

GOAL
As Specified

BACKEND
CL-AtSe

STATISTICS
Analysed : 0 states
Reachable : 0 states
Translation: 0.10 seconds
Computation: 0.00 seconds
```

Fig. 10. Simulated result of the proposed protocol in Cl-AtSe back-end.

4.1. Basic rules of the BAN logic model

- $P \;|\equiv X$: P believes X, or P would be entitled to believe X. In particular, P can take X as true.
- $P \lhd X$: P sees X. P has received some message X and is capable of reading and repeating it (Seeing rule).
- $P \;|\sim X$: P once said X. P at some time sent a message including the statement X. It is not known whether this is a replay, though it is known that P believed X when he sent it.
- $P \Rightarrow X$: P has jurisdiction over X. The principal P is an authority on X and should be trusted on this matter.
- $\sharp(X)$: The message X is fresh.
- (X, Y): The formulae X or Y is one part of the formulae (X, Y).
- $\langle X\rangle_Y$: The formulae X combined with the formulae Y.
- $\{X\}_K$: The formulae X is encrypted under the key K.
- $(X)_K$: The formulae X is hashed with the key K.
- $P \overset{K}{\longleftrightarrow} Q$: Principals P and Q communicate via shared key K.
- $P \overset{X}{\rightleftharpoons} Q$: The formula X is a secret known only to P and Q, and possibly to principals trusted by them.
- $\overset{K}{\mapsto} P$: Principal P has K as its public key.
- SK: The session key used in the current session.

4.2. BAN logic rules

- **Message-meaning rule**: $\frac{P|\equiv P\overset{K}{\rightleftharpoons}Q,\ P\lhd\langle X\rangle_K}{P|\equiv Q|\sim X}$
  If the principal P believes that the secret K is shared with Q and sees $\langle X\rangle_K$, then P believes that Q once said X.
- **Freshness-conjuncatenation rule**: $\frac{P|\equiv\sharp(X)}{P|\equiv\sharp(X,Y)}$
  If the principal believes that X is fresh, then the principal P believes freshness of (X, Y).
- **Belief rule**: $\frac{P|\equiv(X),P|\equiv Y}{P|\equiv(X,Y)}$
  If the principal P believes X and Y, then the principal P believes (X, Y).
- **Nonce-verification rule**: $\frac{P|\equiv\sharp(X),\ P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$
  If the principal P believes that X is fresh and the principal Q once sent X, then principal P believes that Q believes X.
- **Jurisdiction rule**: $\frac{P|\equiv Q\Rightarrow X,\ P|\equiv Q|\equiv X}{P|\equiv X}$
  If the principal believes that Q has jurisdiction over X and Q believes X, then P believes that X is true.
- **Session key rule**: $\frac{P|\equiv\sharp(X),P|\equiv Q|\equiv X}{P|\equiv P\overset{K}{\longleftrightarrow}Q}$
  If the principal P believes that the session key is fresh and the principal P and Q believes X, which are the necessary parameters of the session key, then principal P believes that s/he shares the session key K with Q.

The proposed protocol should accomplish the following goals that should be proved to validate security.

- **Goal 1**: $GW \;|\equiv GW \overset{SK}{\longleftrightarrow} U_i$
- **Goal 2**: $GW \;|\equiv U_i \;|\equiv GW \overset{SK}{\longleftrightarrow} U_i$
- **Goal 3**: $GW \;|\equiv GW \overset{SK}{\longleftrightarrow} SN_j$
- **Goal 4**: $GW \;|\equiv SN_j \;|\equiv GW \overset{SK}{\longleftrightarrow} SN_j$
- **Goal 5**: $SN_j \;|\equiv SN_j \overset{SK}{\longleftrightarrow} GW$
- **Goal 6**: $SN_j \;|\equiv GW \;|\equiv SN_j \overset{SK}{\longleftrightarrow} GW$
- **Goal 7**: $U_i \;|\equiv U_i \overset{SK}{\longleftrightarrow} GW$
- **Goal 8**: $U_i \;|\equiv GW \;|\equiv U_i \overset{SK}{\longleftrightarrow} GW$.

The idealized form of the proposed protocol are as follows.

- **M1**: $U_i \rightarrow GW: TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 : \langle R_1\rangle_{B_i}$
- **M2**: $GW \rightarrow SN_j : M_3, M_4, M_5 : \langle R_2\rangle_{SK_{GW-SN_j}}$
- **M3**: $SN_j \rightarrow GW : M_7, M_8 : \langle R_3\rangle_{SK_{GW-SN_j}}$
- **M4**: $GW \rightarrow U_i : M_8, M_9, M_{10}, M_{11} : \langle(R_1, R_2)\rangle_{B_i}$.

4.3. Initial assumptions of the protocol

- **A1**: $U_i \;|\equiv \sharp(R_1, R_2, R_3)$
- **A2**: $GW \;|\equiv \sharp(R_2, R_1, R_3)$
- **A3**: $SN_j \;|\equiv \sharp(R_3, R_2)$
- **B1**: $SN_j \;|\equiv GW \Rightarrow R_2$
- **B2**: $GW \;|\equiv SN_j \Rightarrow R_3$
- **B3**: $GW \;|\equiv U_i \Rightarrow R_1$
- **B4**: $U_i \;|\equiv GW \Rightarrow (R_2, R_3)$
- **C1**: $U_i \;|\equiv U_i \overset{B_i}{\longleftrightarrow} GW$
- **C2**: $GW \;|\equiv GW \overset{SK_{GW-SN_j}}{\longleftrightarrow} SN_j$.

To prove the mentioned goals, the idealized form is analyzed using BAN logic rules and assumptions.

- **M1**: $U_i \rightarrow GW: TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 : \langle R_1\rangle_{B_i}$
- Using *seeing rule*,
  S1: $GW \lhd TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 : \langle R_1\rangle_{B_i}$
- Using **C1**, **S1** and *message meaning rule*,
  S2: $GW \;|\equiv U_i \;|\sim R_1$
- Using **A2**, **S2** and *freshness-conjuncatenation* rule and *nonce verification rule*,
  S3: $GW \;|\equiv U_i \;|\equiv R_1$, where R_1 is essential information to compute session key in the proposed protocol.
- Using **B3**, **S3** and *jurisdiction rule*,
  S4: $GW \;|\equiv R_1$
- Using **A2**, **S3** and *session key rule*,
  S5: $GW \;|\equiv GW \overset{SK}{\longleftrightarrow} U_i$ **(Goal 1)**
- Using **A2**, **S5** and *nonce verification rule*,
  S6: $GW \;|\equiv U_i \;|\equiv GW \overset{SK}{\longleftrightarrow} U_i$ **(Goal 2)**
- **M2**: $GW \rightarrow SN_j : M_3, M_4, M_5 : \langle R_2\rangle_{SK_{GW-SN_j}}$
- Using *seeing rule*,
  V1: $SN_j \lhd M_3, M_4, M_5 : \langle R_2\rangle_{SK_{GW-SN_j}}$
- Using **C2**, **V1** and *message meaning rule*,
  V2: $SN_j \;|\equiv GW \;|\sim R_2$
- Using **A3**, **V2** and *freshness-conjuncatenation rule* and *nonce verification rule*,
  V3: $SN_j \;|\equiv GW \;|\equiv R_2$, where R_2 is essential information to calculate session key in the proposed protocol.

- Using **B1**, **V3** and *jurisdiction rule*,
  V4: $SN_j \mid\equiv R_2$
- Using **A3**, **V3** and *session key rule*,
  V5: $SN_j \mid\equiv SN_j \xleftrightarrow{SK} GW$ **(Goal 5)**
- Using **A3**, **V5** and *nonce verification rule*,
  V6: $SN_j \mid\equiv GW \mid\equiv SN_j \xleftrightarrow{SK} GWj$ **(Goal 6)**
- **M3**: $SN_j \rightarrow GW : M_7, M_8 : \langle R_3 \rangle_{SK_{GW-SN_j}}$
- Using *seeing rule*,
  Q1: $GW \triangleleft M_7, M_8 : \langle R_3 \rangle_{SK_{GW-SN_j}}$
- Using **C2**, **Q1** and *message meaning rule*,
  Q2: $GW \mid\equiv GW \mid\sim R_3$
- Using **A2**, **Q2** and *freshness-conjuncatenation rule* and *nonce verification rule*,
  Q3: $GW \mid\equiv SN_j \mid\equiv R_3$, where R_3 is the essential information to calculate session key in the proposed protocol.
- Using **B2**, **Q3** and *jurisdiction rule*,
  Q4: $GW \mid\equiv R_3$
- Using **A2**, **Q3** and *session key rule*,
  Q5: $GW \mid\equiv GW \xleftrightarrow{SK} SN_j$ **(Goal 3)**
- Using **A2**, **Q5** and *nonce verification rule*,
  Q6: $GW \mid\equiv SN_j \mid\equiv GW \xleftrightarrow{SK} SN_j$ **(Goal 4)**
- **M4**: $GW \rightarrow U_i : M_8, M_9, M_{10}, M_{11} : \langle (R_1, R_2) \rangle_{B_i}$
- Using *seeing rule*,
  W1: $U_i \triangleleft M_8, M_9, M_{10}, M_{11} : \langle (R_1, R_2) \rangle_{B_i}$
- According to **C1**, **W1** and *message meaning rule*,
  W2: $U_i \mid\equiv GW \mid\sim (R_2, R_3)$
- Using **A1**, **W2** and *freshness-conjuncatenation rule* and *nonce verification rule*,
  W3: $U_i \mid\equiv GW \mid\equiv (R_2, R_3)$, where (R_2, R_3) is the essential information to calculate session key in the proposed protocol.
- Using **B4**, **W3** and *jurisdiction rule*,
  W4: $U_i \mid\equiv (R_2, R_3)$
- Using **A1**, **W3** and *session key rule*,
  W5: $U_i \mid\equiv U_i \xleftrightarrow{SK} GW$ (**Goal 7**)
- Using **A1**, **W5** and *nonce verification rule*,
  W6: $U_i \mid\equiv GW \mid\equiv U_i \xleftrightarrow{SK} GW$ (**Goal 8**).

We successfully prove the above-mentioned goals using *BAN* logic model and hence, the proposed protocol claims mutual authentication and session key agreement.

5. Further security analysis

This section illustrates by demonstrating security analysis of the proposed protocol that it can resist all the attacks. In this regard, the following assumptions have been made [2,6,10,20].

(i) The public messages are transmitted through insecure channel and the adversary $\mathcal{A}$ can intercept, delete, modify, re-route, re-send the transmitted message over insecure networks. However, $\mathcal{A}$ cannot intercept any information from the secure channel.

(ii) In password-based user authentication protocol, user uses dictionary word as password and identity and $\mathcal{A}$ cannot guess them in polynomial time. Let, $A_i = h(ID_i \parallel PW_i)$ is known to $\mathcal{A}$, then it is infeasible to justify the correctness of the guessed identity and password using A_i in polynomial time.

(iii) In password-based user authentication protocol, it is assumed that the secret key and random numbers are sufficiently large. An adversary $\mathcal{A}$ has no ability to guess these information in polynomial time.

(iv) Suppose $A_i = B_i \oplus C_i$ is known to $\mathcal{A}$. However, $\mathcal{A}$ cannot find B_i or C_i from A_i in polynomial time.

(v) The guessing probability for n characters is approximately $\frac{1}{2^{6n}}$ [31], where the identity/password is composed with n characters.

(vi) All the confidential information stored in the mobile device are in plaintext form. Therefore, upon getting the mobile device of an user, $\mathcal{A}$ can obtain all the confidential information stored the mobile device.

Proposition 1. *The proposed protocol can withstand mobile device stolen attack.*

Proof. In this attack, $\mathcal{A}$ attempts to extract confidential information and then tries to misuse these information. We assume that $\mathcal{A}$ has got the mobile device of a legal user U_i and extracted all the information from it. However, the following descriptions show that the proposed protocol can withstand this attack.

- $\mathcal{A}$ knows $\langle TID_i, Reg_i, A_i, C_i, h(\cdot) \rangle$, where $Reg_i = h(ID_i \parallel R_i \parallel HPW_i)$, $A_i = R_i \oplus HPW_i$, $B_i = h(ID_i \parallel R_i \parallel K)$, $C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i)$, $D_i = R_i \oplus h(TID_i \parallel K)$. Note that Reg_i is protected by $h(\cdot)$. Therefore, $\mathcal{A}$ is not capable to extort any information owing to the one-way property of $h(\cdot)$. The probability of guessing ID_i and PW_i using Reg_i is approximately equal to $\frac{1}{2^{12n+160}}$, which is negligible. On the other hand, $\mathcal{A}$ is unable to compute HPW_i without knowing R_i. The confidential information in the mobile device is B_i, which is used to compute C_i. $\mathcal{A}$ cannot compute B_i without knowing $\langle ID_i, R_i, HPW_i \rangle$. In addition, computation of R_i is not feasible without knowing the secret key of GW.
- $\mathcal{A}$ may attempt to impersonate U_i using the mobile device information. In order to do that, $\mathcal{A}$ has to send the message $\langle TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 \rangle$ to GW and if it is verified, $\mathcal{A}$ is successful, where $M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1)$, $M_2 = h(R_i \parallel T_1) \oplus R_1$. However, $\mathcal{A}$ needs $\langle B_i, ID_i \rangle$ and R_i to compute M_1 and M_2, respectively. However, we demonstrate that $\mathcal{A}$ cannot compute these information without B_i.

Therefore, $\mathcal{A}$ cannot launch medical professional impersonation attack using mobile device information. □

Proposition 2. *The proposed protocol preserves anonymity of the medical professional.*

Proof. User anonymity implies that outsider person is not capable to know or guess identity using public information of the protocol. In order to violate the anonymity, the adversary first traps all the messages transmitted between the participants during the protocol execution and then tries to guess the identity of the user. We claim that $\mathcal{A}$ is unable to break the anonymity of the proposed protocol using public messages. The elucidation is given below.

- We assume that $\mathcal{A}$ traps the login message $\langle TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1 \rangle$, where $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \parallel HPW_i^*)$, $CID_i = ID_i \oplus h(TID_i \parallel R_i^* \parallel T_1)$, $M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1)$, $M_2 = h(R_i \parallel T_1) \oplus R_1$. $\mathcal{A}$ cannot compute ID_i from CID_i and M_1 without knowing R_i and $\langle B_i, R_1 \rangle$, respectively. However, $\mathcal{A}$ can verify the guessed identity ID_i^g using these information. To examine the correctness of the guessed identity using CID_i and M_1, the probability would be approximately equal to $\frac{1}{2^{6n+128}}$ and $\frac{1}{2^{12n+320}}$, respectively.
- We assume that $\mathcal{A}$ traps the message $\langle M_3, M_4, M_5 \rangle$, where $M_3 = h(h(h(ID_i \parallel R_1^* \parallel R_2) \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2)$, $M_4 = h(ID_i \parallel R_1 \parallel R_2) \oplus SK_{GW-SN_j}$, $M_5 = R_2 \oplus h(SK_{GW-SN_j})$. Note that ID_i is used to compute M_3 and M_4, which are protected by $h(\cdot)$. Therefore, the extraction of ID_i using these information is computationally infeasible owing to property of $h(\cdot)$.
- The identity ID_i of U_i is not directly involved in $\langle M_7, M_8 \rangle$, where $M_7 = h(SK \parallel R_3 \parallel SK_{GW-SN_j})$, $M_8 = h(R_2) \oplus R_3$. Therefore, $\mathcal{A}$ cannot derive ID_i if he/she traps $\langle M_7, M_8 \rangle$ during protocol run.

- We supposed that $\mathcal{A}$ traps $\langle M_8, M_9, M_{10}, M_{11}\rangle$ during the protocol run, where $M_9 = R_2 \oplus h(ID_i \parallel R_1), M_{10} = h(ID_i \parallel SK' \parallel R_3'), M_{11} = TID_i' \oplus h(R_2 \oplus R_3)$. The identity ID_i is protected by $h(\cdot)$ in $\langle M_9, M_{10}\rangle$ and the extraction is computationally infeasible. In addition, probability of guessing ID_i is $\frac{1}{2^{6n+320}}$, which is not feasible in polynomial time. □

Proposition 3. *The untraceibility attack is fully protected in the proposed protocol.*

Proof. The untraceibility means that an adversary $\mathcal{A}$ cannot trace the medical professional U_i from the available login and authentication messages. If $\mathcal{A}$ can trace U_i after intercepting the transmitted message, the protocol is said to be susceptible to the untraceibility attack. With his attack, the main objective of $\mathcal{A}$ is to reveled the identity ID_i of U_i.

In this respect, we believe that the proposed protocol is secure against the untraceibility attack. The explanation is given as follows. We assume that $\mathcal{A}$ traps the login and authentication messages $\langle TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1\rangle$ and $\langle TID_i', ID_{SN_j}, CID_i', M_1', M_2', T_1'\rangle$ during protocol run and compares them to find a match, where $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \parallel HPW_i^*), CID_i = ID_i \oplus h(TID_i \parallel R_i^* \parallel T_1)$, $M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1), M_2 = h(R_i \parallel T_1) \oplus R_1$. However, all of these messages are fresh due to the timestamp T_1 and the random numbers $\langle R_1, R_2, R_3\rangle$. Therefore, $\mathcal{A}$ cannot trace U_i after intercepting the login and authentication messages of any session. □

Proposition 4. *The off-line password guessing attack is fully protected in the proposed protocol.*

Proof. In general, the user chooses password from a small dictionary, which is low-entropy in nature and it can easily be guessed in polynomial time if a robust approach is not followed. We assume that $\mathcal{A}$ has got the mobile device of U_i and extracted the information $\langle TID_i, Reg_i, A_i, C_i, h(\cdot)\rangle$, where $Reg_i = h(ID_i \parallel R_i \parallel HPW_i), A_i = R_i \oplus HPW_i, B_i = h(ID_i \parallel R_i \parallel K), C_i = B_i \oplus h(ID_i \oplus R_i \oplus HPW_i), D_i = R_i \oplus h(TID_i \parallel K)$. In the proposed protocol, PW_i is used to compute $HPW_i = h(ID_i \oplus PW_i)$. Using the mobile device information, $\mathcal{A}$ is unable to compute HPW_i. In addition, $\mathcal{A}$ may guess PW_i from $\langle Reg_i, A_i, C_i\rangle$, however, the probability is approximately equal to $\frac{1}{2^{12n+160}}, \frac{1}{2^{6n+160}}$ and $\frac{1}{2^{12n+1344}}$, respectively. Hence, $\mathcal{A}$ cannot get success to guess the password PW_i of U_i in polynomial time. □

Proposition 5. *The random numbers are fully protected in the proposed protocol.*

Proof. Here, we demonstrate that $\langle R_1, R_2, R_3\rangle$ cannot be retrieved by $\mathcal{A}$ from the intercepted public messages. Note that R_1 cannot be computed from $\langle M_1, M_2\rangle$ owing to one-way property of $h(\cdot)$, where $M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1), M_2 = h(R_i \parallel T_1) \oplus R_1$. By the same reason, $\mathcal{A}$ cannot retrieve R_2 from M_3 and M_4, where $M_3 = h(h(h(ID_i \parallel R_1^* \parallel R_2) \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2), M_4 = h(ID_i \parallel R_1 \parallel R_2) \oplus SK_{GW-SN_j}$. In addition, $\mathcal{A}$ needs to know SK_{GW-SN_j} to compute R_2 from $M_5 = R_2 \oplus h(SK_{GW-SN_j})$. $\mathcal{A}$ cannot extract R_3 from M_7 without R_2. $\mathcal{A}$ cannot extract any random number from the message $\langle M_8, M_9, M_{10}, M_{11}\rangle$ due to $h(\cdot)$, where $M_9 = R_2 \oplus h(ID_i \parallel R_1), M_{10} = h(ID_i \parallel SK' \parallel R_3'), M_{11} = TID_i' \oplus h(R_2 \oplus R_3)$. □

Proposition 6. *The medical professional impersonation attack is fully protected in the proposed protocol.*

Proof. In this attack, $\mathcal{A}$ makes an effort to masquerade U_i and if it happens, the system will suffer from numerous problems. Assume that $\mathcal{A}$ captures the message $\langle TID_i, ID_{SN_j}, CID_i, M_1, M_2, T_1\rangle$ and attempts to generate another fabricated message by incorporating new random number(s) and timestamp so that forged message can be accepted by GW, where $B_i^* = C_i \oplus h(ID_i \oplus R_i^* \parallel HPW_i^*)$, $CID_i = ID_i \oplus h(TID_i \parallel R_i^* \parallel T_1), M_1 = h(ID_i \parallel B_i^* \parallel R_1 \parallel T_1)$, $M_2 = h(R_i \parallel T_1) \oplus R_1$. $\mathcal{A}$ can generate random nonce and current timestamp, however, to compute CID_i, M_1 and M_2, he/she needs ID_i, B_i and R_i, respectively. Therefore, $\mathcal{A}$ cannot impersonate medical professional U_i. □

Proposition 7. *The gateway node impersonation attack is fully protected in the proposed protocol.*

Proof. Similar to Proposition 6, $\mathcal{A}$ may also make an effort to impersonate GW. Thus, $\mathcal{A}$ has to compute all the valid messages generated by GW. During the protocol execution, GW transmits $\langle M_3, M_4, M_5\rangle$ and $\langle M_8, M_9, M_{10}, M_{11}\rangle$, respectively, where $M_3 = h(h(h(ID_i \parallel R_1^* \parallel R_2) \parallel \text{“1”}) \parallel SK_{GW-SN_j} \parallel R_2), M_4 = h(ID_i \parallel R_1 \parallel R_2) \oplus SK_{GW-SN_j}, M_5 = R_2 \oplus h(SK_{GW-SN_j})$ to SN_j, $M_9 = R_2 \oplus h(ID_i \parallel R_1), M_{10} = h(ID_i \parallel SK' \parallel R_3'), M_{11} = TID_i' \oplus h(R_2 \oplus R_3)$. $\mathcal{A}$ is not able to compute the messages $\langle M_3, M_4, M_5\rangle$ and $\langle M_8, M_9, M_{10}, M_{11}\rangle$ without $\langle ID_i, SK_{GW-SN_j}\rangle$ and $\langle ID_i, SK\rangle$, respectively. Therefore, the proposed protocol can withstand the gateway node impersonation attack. □

Proposition 8. *The session key is fully protected in the proposed protocol.*

Proof. During the protocol execution, session key is negotiated between the participants, which is used to provide secure message communication. Thus, the protection of the session key is necessary. The security of the session key $SK = h(h(ID_i \parallel R_1 \parallel R_2) \parallel R_2 \parallel R_3)$ depends on the strength of $h(\cdot)$. In Proposition 5, we demonstrated that $\mathcal{A}$ cannot compute the random numbers $\langle R_1, R_2, R_3\rangle$ and Proposition 2 analyzed that the guessing of ID_i is computationally infeasible. Therefore, the session key SK of the proposed scheme is secured from the adversary. □

Proposition 9. *The known key security of the session key is ensured in the proposed protocol.*

Proof. It signifies that if the session key of a session is disclosed by some means, however, none of the previous and future session keys are known to $\mathcal{A}$. Suppose the session key $SK = h(h(ID_i \parallel R_1 \parallel R_2) \parallel R_2 \parallel R_3)$ of current session is known to $\mathcal{A}$, however, he/she cannot compute none of the past and future session keys using SK. Since the session key is protected by $h(\cdot)$ and the random numbers $\langle R_1, R_2, R_3\rangle$ are different in each session. □

Proposition 10. *The mutual authentication property is ensured in the proposed protocol.*

Proof. In client–server communication over open channel, mutual authentication between client and server is extremely essential in order to avoid impersonation attack. In Step 3 of the login phase (see Section 2.4), GW first authenticates U_i and then start further computation. In Step 5 (see Section 2.4), SN_j authenticates U_i and GW, and then GW authenticates SN_j in Step 6. Finally, U_i authenticates GW and SN_j in Step 7. Therefore, the mutual authentication between the legal protocol participants is ensured in the proposed protocol. □

Proposition 11. *The proposed protocol achieves the session key verification property.*

Proof. In the proposed protocol, after performing mutual authentication, all the participants negotiate a common session key between them. However, it is essential to verify whether session key is same for all entities. In Step 6 and Step 7 (see Section 2.4), GW and U_i ensure the exactness of the session key by examining whether $M_7'? = M_7$ and $M_{10}^*? = M_{10}$ hold. □

Table 2
Computation cost comparison of the login and authentication phases of different protocols.

Protocol	Computation cost for U_i	Computation cost for *GW*	Computation cost for SN_j	Overall computation cost	Overall execution time (ms)
Kumar et al. [21]	$4T_h + 2T_s$	$T_h + 3T_s$	$T_h + 2T_s$	$6T_h + 7T_s$	0.9145
He et al. [22]	$4T_h + 2T_s$	$2T_h + 5T_s$	$T_h + 2T_s$	$7T_h + 9T_s$	1.1755
Wu et al. [23]	$10T_h + 2T_s$	$6T_h + 5T_s$	$4T_h + T_s$	$20T_h + 8T_s$	1.0504
Khan et al. [24]	$6T_h + T_s$	$7T_h + T_s$	$7T_h$	$20T_h + 2T_s$	0.5212
Li et al. [25]	$6T_h + 2T_s$	$7T_h + 6T_s$	$5T_h + 2T_s$	$18T_h + 10T_s$	1.3102
Proposed	$12T_h$	$16T_h$	$6T_h$	$34T_h$	0.0136

Table 3
Execution time comparison of the sensor node SN_j of the proposed protocol with related protocols.

Protocol	Computation cost	Execution time (ms)
Kumar et al. [21]	$T_h + 2T_s$	0.2610
He et al. [22]	$T_h + 2T_s$	0.2610
Wu et al. [23]	$4T_h + T_s$	0.2622
Khan et al. [24]	$7T_h$	0.0028
Li et al. [25]	$5T_h + 2T_s$	0.2626
Proposed	$6T_h$	0.0024

6. Performance evaluation and comparative analysis

This section provides the performance evaluation of the proposed protocol and compares it with the other existing protocols proposed in [21–25]. We considered only two cryptographic operations such as, hash function (T_h) and symmetric key en/decryption (T_s). In [32], the approximate execution time of the different cryptographic operations are calculated using *MIRACL*, which is a *C/C++* library. For this experiment, the authors have considered the *32*-bit Windows *7* OS, the Visual *C++ 2008* S/W, a *160*-bit prime field F_p, a *1024*-bit cyclic group, *AES* algorithm and *SHA-1* hash function. The approximate execution time of the *SHA-1* and *AES* functions are obtained as $T_h \approx 0.0004$ ms and $T_s \approx 0.1303$ ms, respectively. The registration phase of the medical professional executes only once and thus, we can ignore it in the comparison. On the other hand, execution of the password change phase depends on medical professional's demand and generally it executes periodically due to security reasons. Hence, we also include the password change phase in comparison.

In wireless sensor networks, the main challenge is to optimize the energy consumption of the sensor nodes. Basically, the energy of the sensor nodes are dependent on how much cryptographic operations are performed and how much data is transmitted to the target entity. In Table 2, we provided computation cost separately for medical professional, gateway node and sensor node of the login and authentication phase and the execution time in milliseconds (ms). We provided the computation cost of the sensor node in Table 2. The proposed authentication protocol achieves computation cost efficiency against the protocols in [21–25]. The proposed protocol takes 0.0136 ms, whereas the protocols in [21–25] take 0.9145 ms, 0.5212 ms, 1.1755 ms, 1.3102 ms and 1.0504 ms, respectively. The Table 2 also highlights that the proposed protocol consumes less energy (execution time) of the sensor node than the protocols in [21–23,25].

Table 3 provides computation cost of the sensor node of different protocols including ours. The life-time of the sensor node depends on (i) computing parameters, (ii) length of the transmitted data (bits) and (iii) length of the receiving data (bits). We observed in Table 3 that the proposed protocol takes less computation time compared to other protocols. Therefore, the proposed protocol achieves better performance in terms of energy consumption of the sensor node. In Table 4, we provided the time complexity of the password change phase of the proposed protocol and the protocols in [21–23,25]. For comparison, we considered the length of the random number, password, identity and timestamp are 64 bits each. In addition, message digest of the hash function (SHA-1) takes 160 bits and the symmetric key en/decryption (AES-256) produces 256 bits. The proposed protocol achieves computation cost efficiency in compared with the protocols in [23, 25]. Furthermore, the protocol in [23] only takes communication cost of 1248 bits during the password change phase. On the other hand, the protocol in [22] does not verify login identity and password before updating the password. Therefore, the protocol in [22] suffers from different security pitfalls as mentioned in [6].

In Table 5, we provided the total communication cost for the login and authentication phases and the number of communications of the proposed protocol and related protocols proposed in [21–25]. From this table, we found that the proposed protocol takes little more communication cost and the number of message communications is also more than the protocols propose in [21–23]. However, the protocols propose in [21–23] are not suitable due to high energy consumption of the sensor node.

In Table 6, we provided the number of bits transmitted and received by the sensor node during protocol execution, which is important to measure the life-time of the sensor node. In Table 6, we found that the sensor node of the proposed protocol takes almost same energy in one authentication cycle compared with the protocols proposed in [21,22,24,25]. In this context, we point out that the protocol in [23] is not efficient as it needs high energy consumptions. The sensor node of the protocols in [21–23] transmits the message over long distance to the medical professional and thus, the energy consumption of these protocols by the sensor node is high.

7. Conclusion

The WMSN incorporates the wireless sensor network and mobile communication network. Recently, WMSN is popularly used in patient monitoring system to boosts the quality of life of the patients. In patient monitoring system, the sensor devices sense various health conditions of a patient, and send the sensitive health data to the medical professional through a gateway node of the WMSN. The patient data is transmitted through an open channel and the protection of it is a big concern in health-care applications. To make secure the patient data over WMSN, in this article, we have designed an architecture to support health monitoring system for WMSN and then proposed a robust anonymous authentication protocol for WMSN. The AVISPA software is used and the proposed protocol is simulated on it to ensure the security attack resilience of the proposed protocol, and the results obtained confirm that the protocol is robust against the known threats. Moreover, the mutual authentication verification of the protocol has been analyzed using the BAN logic model. Moreover, we have proved that the proposed protocol is robust against the relevant and known security attacks. We have also measured the complexity of the proposed protocol and compared against the existing protocols. The comparative analysis ensured that the proposed protocol is more cost-effective and robust and than the existing protocols.

In the future, we would like to implement the proposed protocol in Internet-of-Things and cloud environments. Furthermore, the provable security of the proposed protocol will be examined in a computational model and the breaching probability of the adversary to break the proposed protocol will be estimated.

Table 4
The comparative analysis of the proposed protocol with existing protocols for the password change phase.

Protocol	Computation cost	Execution time (ms)	Communication cost (bits)	Identity and password verification during login
Kumar et al. [21]	$3T_h$	0.0012	0000	Yes
He et al. [22]	$2T_h$	0.0008	0000	No
Wu et al. [23]	$8T_h + 3T_s$	0.3941	1284	Yes
Khan et al. [24]	$3T_h$	0.0012	0000	Yes
Li et al. [25]	$6T_h$	0.0024	0000	Yes
Proposed	$5T_h$	0.0020	0000	Yes

Table 5
The comparative analysis of the proposed protocol with existing protocols with respect to the overall communication cost.

Protocol	Communication cost (bits)	Number of communications	Communication structure
Kumar et al. [21]	1216	3	$U_i \rightarrow GW \rightarrow SN_j \rightarrow U_i$
He et al. [22]	1216	3	$U_i \rightarrow GW \rightarrow SN_j \rightarrow U_i$
Wu et al. [23]	2048	3	$U_i \rightarrow GW \rightarrow SN_j \rightarrow U_i$
Khan et al. [24]	1536	4	$U_i \rightarrow GW \rightarrow SN_j \rightarrow GW \rightarrow U_i$
Li et al. [25]	1546	4	$U_i \rightarrow GW \rightarrow SN_j \rightarrow GW \rightarrow U_i$
Proposed	2112	4	$U_i \rightarrow GW \rightarrow SN_j \rightarrow GW \rightarrow U_i$

Table 6
The comparative analysis of the proposed protocol with existing protocols with respect to the communication cost of the sensor node.

Protocol	Transmit (bits)	Receive (bits)
Kumar et al. [21]	320	320
He et al. [22]	320	320
Wu et al. [23]	800	576
Khan et al. [24]	320	470
Li et al. [25]	320	320
Proposed	320	480

Acknowledgments

SK Hafizul Islam is thankful to the BITS Pilani, Rajasthan for providing the OPERA award to support this research work. The authors are also thankful to the Deanship of Scientific Research at King Saud University for its funding this Prolific Research Group (PRG-1436-16).

References

[1] S.H. Islam, G.P. Biswas, Design of two-party authenticated key agreement protocol based on ecc and self-certified public keys, Wirel. Pers. Commun. 82 (4) (2015) 2727–2750.
[2] R. Amin, G.P. Biswas, A novel user authentication and key agreement protocol for accessing multi-medical server usable in tmis, J. Med. Syst. 39 (3) (2015) 1–17.
[3] S. Kumari, S.A. Chaudhry, F. Wu, X. Li, M.S. Farash, M.K. Khan, An improved smart card based authentication scheme for session initiation protocol, Peer-to-Peer Netw. Appl. (2015) 1–14. http://dx.doi.org/10.1007/s12083-015-0409-0.
[4] S.A. Chaudhry, M.S. Farash, H. Naqvi, S. Kumari, M.K. Khan, An enhanced privacy preserving remote user authentication scheme with provable security, Secur. Commun. Netw. 8 (18) (2015) 3782–3795.
[5] G. Li, Q. Jiang, F. Wei, C. Ma, A new privacy-aware handover authentication scheme for wireless networks, Wirel. Pers. Commun. 80 (2) (2015) 581–589.
[6] R. Amin, G.P. Biswas, A secure three-factor user authentication and key agreement protocol for tmis with user anonymity, J. Med. Syst. 39 (8) (2015) 1–19.
[7] R. Amin, G.P. Biswas, An improved rsa based user authentication and session key agreement protocol usable in tmis, J. Med. Syst. 39 (8) (2015) 1–14.
[8] R. Amin, S.H. Islam, G.P. Biswas, M.K. Khan, N. Kumar, An efficient and practical smart card based anonymity preserving user authentication scheme for tmis using elliptic curve cryptography, J. Med. Syst. 39 (11) (2015) 1–18.
[9] S.H. Islam, R. Amin, G.P. Biswas, M.S. Farash, X. Li, S. Kumari, An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments, J. King Saud Univ. Comput. Inf. Sci. (2015) http://dx.doi.org/10.1016/j.jksuci.2015.01.004.
[10] R. Amin, G.P. Biswas, Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment, Wirel. Pers. Commun. (2015) 1–24. http://dx.doi.org/10.1007/s11277-015-2616-7.
[11] S.H. Islam, Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps, Inform. Sci. 312 (2015) 104–130.
[12] S. Kumari, M.K. Khan, M. Atiquzzaman, User authentication schemes for wireless sensor networks: A review, Ad Hoc Networks 27 (2015) 159–194.
[13] S. Kumari, M.K. Khan, X. Li, F. Wu, Design of a user anonymous password authentication scheme without smart card, Int. J. Commun. Syst. 29 (3) (2016) 441–458. http://dx.doi.org/10.1002/dac.2853.
[14] S. Kumari, M.K. Khan, X. Li, An improved remote user authentication scheme with key agreement, Comput. Electr. Eng. 40 (6) (2014) 1997–2012.
[15] S. Kumari, M.K. Khan, More secure smart card-based remote user password authentication scheme with user anonymity, Secur. Commun. Netw. 7 (11) (2014) 2039–2053.
[16] S. Kumari, M.K. Gupta, M.K. Khan, X. Li, An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement, Secur. Commun. Netw. 7 (11) (2014) 1921–1932.
[17] T. Maitra, R. Amin, D. Giri, P.D. Srivastava, An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card, Int. J. Netw. Secur. 18 (3) (2016) 553–564.
[18] R. Amin, S.H. Islam, G.P. Biswas, M.K. Khan, X. Li, Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems, J. Med. Syst. 39 (11) (2015) 1–21.
[19] D. He, N. Kumar, N. Chilamkurti, A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks, Inform. Sci. 321 (10) (2015) 263–277.
[20] R. Amin, G.P. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Networks 36 (2016) 58–80.
[21] P. Kumar, S.-G. Lee, H.-J. Lee, E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks, Sensors 12 (2) (2012) 1625–1647.
[22] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, S.-S. Yeo, Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Multimedia Syst. 21 (1) (2013) 49–60.
[23] F. Wu, L. Xu, S. Kumari, X. Li, An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks, Multimedia Syst. (2015) 1–11. http://dx.doi.org/10.1007/s00530-015-0476-3.
[24] M.K. Khan, S. Kumari, An improved user authentication protocol for healthcare services via wireless medical sensor networks, Int. J. Distrib. Sens. Netw. (2014) 10. http://dx.doi.org/10.1155/2014/347169.
[25] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, M.K. Khan, A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity, Secur. Commun. Netw. (2015) http://dx.doi.org/10.1002/sec.1214.
[26] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, The AVISPA Tool for the automated validation of internet security protocols and applications, in: Proceedings of the 17th International Conference on Computer Aided Verification, CAV'05, Edinburgh, Scotland, UK, 2005, pp. 281-285.
[27] S.H. Islam, G.P. Biswas, A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings, J. King Saud Univ. Comput. Inf. Sci. 26 (1) (2014) 55–67.
[28] S.H. Islam, G.P. Biswas, An efficient and secure strong designated verifier signature scheme without bilinear pairings, J. Appl. Math. Inf. 31 (3–4) (2013) 425–441.
[29] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1) (1990) 18–36.
[30] D. Dolev, A.C. Yao, On the security of public key protocols, IEEE Trans. Inform. Theory 29 (2) (1983) 198–208.
[31] Y.-F. Chang, S.-H. Yu, D.-R. Shiao, A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care, J. Med. Syst. 37 (2) (2013) http://dx.doi.org/10.1007/s10916-012-9902-7.
[32] L. Xu, F. Wu, Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care, J. Med. Syst. 39 (2) (2015) 1–9.

Ruhul Amin received his B.Tech. and M.Tech. from West Bengal University of Technology in Computer Science and Engineering in 2009 and 2013, respectively. Currently, he is a pursing Ph.D. in the Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India. He has published many research papers in journals and conference proceedings of international reputes. His current research interests include cryptographic authentication protocol and security in wireless sensor network.

SK Hafizul Islam has received his Ph.D. in Computer Science and Engineering from Indian School of Mines (ISM), Dhanbad, India, under the INSPIRE Fellowship Ph.D. Program, funded by DST, Govt. of India. He did M.Tech in Computer Application from ISM Dhanbad in 2009. He received his B.Sc. (Hons.) in Mathematics and M.Sc. in Applied Mathematics from Vidyasagar University, West Bengal, India in 2004 and 2006, respectively. Presently, he is working as an assistant professor in the Department of Computer Science and Information Systems, Birla Institute of Technology and Science (BITS Pilani), Pilani Campus, Rajasthan 333031, India. He has received the University Gold Medal, S.D. Singha Memorial Endowment Gold Medal and Sabitri Parya Memorial Endowment Gold Medal from Vidyasagar University, West Bengal, India in 2006. He worked as a project associate in the project "Information Security Education and Awareness (ISEA)", No. MIT(2)/2006-08/189/CSE, funded by Ministry of Communication and Information Technology, Govt. of India. He has also received the University Gold Medal from ISM Dhanbad in 2009. He is also the recipient of "**Outstanding Potential for Excellence in Research and Academics** (**OPERA**)" award from BITS Pilani in 2015. He has more than four years of teaching and five years of research experiences, and has published 50 research papers in Journals and Conference proceedings of international reputes. He has served as a reviewer in many reputed international journals and conferences. He is one of the **Associate Editor** of well-reputed journal "**International Journal of Communication System**" published by Wiley with its recent ISI impact factor of 1.106. His research interest includes cryptography and information security. Dr. Islam's homepage can be visited at https://sites.google.com/site/hafi786/.

G.P. Biswas received B.Sc. (Engg.) and M.Sc. (Engg.) degrees in Electrical & Electronics Engineering and Computer Science & Engineering, respectively. He completed his Ph.D. degree in Computer Science & Engineering from Indian Institute of Technology, Kharagpur, India. He is currently working as a professor in the Department of Computer Science & Engineering, Indian School of Mines, Dhanbad, Jharkhand, India. He has around 20 years of teaching and research experiences, and has published more than 100 research articles in journals, conferences and seminar proceedings. His main research interests include cryptography, computer network and security, cellular automata, and VLSI design.

Muhammad Khurram Khan is currently working at the Center of Excellence in Information Assurance (CoEIA), College of Computer & Information Sciences, King Saud University, Saudi Arabia. He is one of the founding members of CoEIA and has also served as the R&D Manager from March 2009 to March 2012. He, along with his team, has developed and successfully managed Cybersecurity Research Program at CoEIA, which turned the center as one of the best centers of excellence in the region. Dr. Khurram is the Editor-in-Chief of well-reputed international journal 'Telecommunication Systems' published by Springer for over 21 years with its recent ISI impact factor of 1.163 (JCR 2013). Furthermore, he is also the full-time editor of several international journals/magazines, including IEEE Communications Magazine; Journal of Network & Computer Applications (Elsevier); IEEE Access; Security & Communication Networks (Wiley); IET Wireless Sensor Systems; PLOS ONE (USA); Journal of Medical Systems (Springer); and Electronic Commerce Research (Springer). Moreover, he is one of the organizing chairs and technical program committee members of more than six dozen international conferences. Dr. Khurram has published over 250 research papers in the journals and conferences of international repute. In addition, he is an inventor of 10 US/PCT patents. He has secured several national and international competitive research grants and awards in the domain of information security. Dr. Khurram is an adjunct professor at Fujian University of Technology, China and an honorary professor at IIIRC, Shenzhen Graduate School, China. His research areas of interest are cybersecurity, digital authentication, biometrics, multimedia security, and technological innovation management. Dr. Khurram is a Fellow of the IET (UK), Fellow of the BCS (UK), Fellow of the FTRA (Korea), senior member of the IEEE, member of the IEEE Technical Committee on Security & Privacy, and member of the IEEE Cybersecurity Community. The homepage of Dr. Khurram can be visited at http://faculty.ksu.edu.sa/khurram.

Neeraj Kumar received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India. He was a Postdoctoral Research Fellow with Coventry University, Coventry, UK. He is currently an associate professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He is the author of more than 100 technical research papers in leading journals and conferences, including the IEEE, Elsevier, Springer, and John Wiley. He has guided many research scholars leading to Ph.D. and M.E./M.Tech. degrees. His research was supported by funding from Tata Consultancy Services, Department of Science and Technology, Council of Scientific and Industrial Research, and University Grant Commission. Some of his research findings are published in top cited journals such as the IEEE Transactions on Industrial Electronics, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Industrial Informatics, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Power Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Consumer Electronics, IEEE Network, IEEE Communications Magazine, IEEE Wireless Communications, IEEE Internet of Things Journal, IEEE Systems Journal, Future Generation Computer Systems, Journal of Network and Computer Applications, and Computer Communications. Dr. Kumar is a member of various professional bodies. He is an associate editor of International Journal of Communication Systems, Wiley.