Future Generation Computer Systems 100 (2019) 882–892

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme

Arezou Ostad-Sharif [a], Hamed Arshad [b], Morteza Nikooghadam [a,*], Dariush Abbasinezhad-Mood [a]

[a] Department of Computer Engineering and Information Technology, Imam Reza University, Mashhad, Iran
[b] Department of Informatics, University of Oslo, Norway

HIGHLIGHTS

- The proposed scheme provides perfect forward secrecy with high efficiency.
- The proposed scheme provides the best storage cost in comparison to the related schemes.
- Cryptanalysis of two protocols has been presented and their challenges have been indicated.
- Comparative efficiency analysis has been provided to show the priority of the proposed protocol.

ARTICLE INFO

Article history:
Received 19 April 2018
Received in revised form 6 March 2019
Accepted 8 April 2019
Available online 21 May 2019

Keywords:
Anonymity
Gateway node
IoT
Key agreement
Three factor authentication
WSN

ABSTRACT

Wireless sensor networks (WSNs) can be deployed in any unattended environment. With new enhancements in internet of things (IoT) technology, authorized users are able to access reliable sensor nodes. By accessing the sensor nodes, they can obtain data and send commands to the nodes. Designing an efficient secure authentication and key agreement scheme is vital because of the resource constrained nature of nodes. During the last decade, several lightweight two-factor or three-factor authentication and key agreement protocols have been proposed to provide secure communication links between users and sensor nodes. However, after careful assessment of these works, we found that two of recently proposed ones, which have tried to improve their previous works, are still susceptible to strong replay attacks or do not provide perfect forward secrecy. Therefore, to address this concern, in this paper, we propose a secure and lightweight authentication and key agreement protocol for IoT based WSNs that is free from the security challenges of previous protocols. Formal security verification of the proposed protocol is presented using the well-known and widely-accepted Automated Validation of Internet Security Protocols and Applications tool. Comparative security and performance evaluations with other related works indicate the superiority of the proposed protocol.

1. Introduction

Wireless sensor networks (WSNs) consist of a series of sensors, which are circumstantially distributed in the selected environment. The location of these sensors is not necessarily defined beforehand. In some cases, the sensors are distributed randomly in dangerous or inaccessible environments [1]. These sensors gather information such as temperature, pressure, sound, quake, and motion. The uses of WSNs are varied which include these applications: agriculture, industrial, health care, disaster management, domestic, surveillance systems, and nuclear power plants [2,3]. Unique features of WSNs include: heterogeneity of nodes, scalability to large scales of deployment, and low cost sensors.

The WSN model, illustrated in Fig. 1, includes sensor nodes, a gateway node, and users. Each sensor node has a processor and sends semi-processed data to the gateway node (GWN). The GWN sends them to the nearest user for subsequent analysis. A user can access any sensor node, which is a part of the WSN, via the GWN. Privacy, message integrity, and user authentication are vital in such environments because the communicating messages can be intercepted, deleted, or re-routed by an adversary [4]. As a result, proper security solutions should be employed to safeguard the communication links [5].

Internet of things (IoT) is any object in the internet substructure which is connected to a developed global dynamic network.

* Corresponding author.
E-mail addresses: arezou.ostadsharif@imamreza.ac.ir (A. Ostad-Sharif), hamedar@ifi.uio.no (H. Arshad), m.nikooghadam@imamreza.ac.ir (M. Nikooghadam), dariush.abbasinezhad@imamreza.ac.ir (D. Abbasinezhad-Mood).

https://doi.org/10.1016/j.future.2019.04.019
0167-739X/

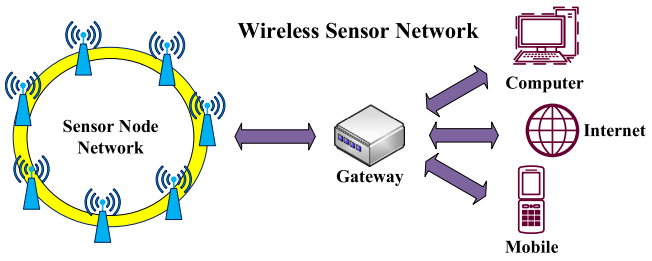

Fig. 1. Communication of data in a WSN through gateway.

The IoT consists of three elements, namely, things, communication networks, and computer systems [6]. Researchers were previously working on new methods and effective approaches on how to better insert WSNs into the IoT situation. In an IoT based WSN, the objects, such as sensor nodes, become smarter as they can communicate conveniently with each other and human beings. This fact has paved the way for creating smart buildings, factories, and in general, smart cities [7,8]. Nevertheless, due to rapid advancements in information and communication technologies, how to address the security and privacy concerns is a big deal in such environments [6,9–11]. The IoT supports novel business models via secure remote access to connected technologies and other devices. In this paper, the design of WSNs are based on a model of IoT in which every sensor node and GWN are inter connected via the Internet. Therefore, the WSN covers a wide-range of application fields and it plays an important role in IoT. As an example, in an industrial IoT, or more specifically, in a smart factory, a large number of sensors are deployed. These sensors communicate with each other and send and receive data to and from powerful computers. A real-world case is the GE's U.S. factory, which utilizes 10,000 smart sensors across 180,000 square feet of its manufacturing space [12]. In this factory, the sensors are connected to a high-speed Ethernet and workers can gather sensing information via the deployed Wi-Fi nodes. These Wi-Fi nodes act as gateways that connect employers to the sensor nodes. Evidently, in such kind of communications, to provide a secure transmission, it is required to devise a secure key agreement protocol [13]. Otherwise, the integrity of communicating messages will be broken and it may lead to some physical harms [7]. In conclusion, to address this vital requirement, this paper suggests a key agreement protocol, which is both efficient and adheres to high-end security metrics.

1.1. Motivation

Even though some researchers have suggested security mechanisms, they are not lightweight enough to cover the needs of the IoT based WSN systems. In this paper, we have proposed a secure and lightweight protocol which provides mutual authentication and key agreement for IoT based WSN environments.

Recently, Amin et al. [14] proposed a lightweight authentication and key agreement protocol with user anonymity for WSNs but Jiang et al. [15] claimed that Amin et al.'s [14] protocol cannot withstand offline password guessing attacks, known-session specific temporary information attacks, and tracking attacks. However, this paper shows that Amin et al.'s protocol [14] is insecure against replay attacks and does not provide perfect forward secrecy. Besides, this paper demonstrates that the protocol of Jiang et al. [15] also does not provide perfect forward secrecy. Furthermore, in order to improve the security of the previous protocols, this paper proposes a new lightweight three factor authentication and key agreement scheme for IoT based WSNs. The security of the proposed protocol is verified using the Automated Validation of Internet Security Protocols and Applications (AVISPA) simulator tool and fully discussed in an informal manner.

1.2. Contribution

The most significant contributions of our work are summarized as below.

- The main novelty of our work is that the proposed protocol provides the perfect forward secrecy while keeps its high efficiency.
- The proposed scheme provides the best storage cost in comparison to the related schemes.
- The security analysis of two state-of-the-art protocols has been presented and their security challenges have been indicated.
- Comparative efficiency analysis in terms of computational, communication, and storage costs has been provided besides formal and informal security analyses to show the priority of the proposed protocol.

1.3. Organization of the paper

After a brief review of related works, the remainder of this paper is organized as follows: we show the drawbacks of Amin et al.'s protocol in Section 3 and also show the drawback of Jiang et al.'s protocol in Section 4. The proposed protocol is presented in Section 5. The results of the simulation of the proposed protocol using the AVISPA tool are given in Section 6, which show the safety of the proposed protocol. A further security discussion is provided in Section 7 and the performance analysis is given in Section 8. Finally, the paper is concluded in Section 9.

2. Related work

To improve WSNs security and functionality, a number of user authentication and key agreement protocols have been suggested so far [16,17]. In the following, we bring a review of the related schemes.

In 2004, Watro et al. [16] suggested a protocol using the Rivest–Shamir–Adleman (RSA) cryptosystem [18] for securing sensor networks. Following, in 2006, Wong et al. [19] proposed a dynamic authentication protocol using the hash function. However, in 2009, because of the incapability of Watro et al.'s protocol [16] to withstand the man-in-the middle attacks, Xu et al. [20] and Song [21] presented two RSA based authentication protocols, which require high amount of memory resulted from the storage of public keys of user and sensor nodes. Vaidya et al. [22] proposed a robust dynamic user authentication and key agreement scheme for WSNs that can overcome the weaknesses of Wong et al.'s protocol [19], such as replay attacks and forgery attacks. At the same year, Das [23] presented a two-factor authentication protocol with high efficiency.

In 2010, He et al. [24] found that the protocol of Das [23] is vulnerable to insider attacks and impersonation attacks. Hence, He et al. [24] introduced an enhanced two-factor user authentication protocol for WSNs. Fan et al. [25] suggested an efficient user authentication protocol for two-tiered WSN that can preserve user anonymity. Yuan et al. [26] introduced a biometric-based user authentication for WSNs at the same year.

In 2011, Yeh et al. [27] suggested an authentication protocol based on elliptic curve cryptosystem (ECC) to address the weaknesses of previous works. Also, Islam and Biswas [17] proposed an ECC based remote mutual authentication protocol that is based on three-way challenge–response handshake technique.

In 2012, Das et al. [28] suggested a new password-based user authentication scheme in hierarchical WSN. Xue et al. [29] suggested a lightweight temporal-credential based mutual authentication and key agreement protocol for WSNs and claimed that

the protocol can withstand stolen smart card attacks, masquerade attacks, and replay attacks.

In 2013, Farash et al. [30] analyzed the security of Cheng and Ma's protocol [31] and found that Cheng and Ma's protocol [31] is vulnerable to forgery attacks. Hence, Farash et al. [30] proposed a new efficient authenticated multiple-key exchange protocol using bilinear pairings. Li et al. [32] analyzed the protocol of Xue et al. [29] and proved that their protocol suffers from stolen verifier, insider, and offline password guessing attacks. Li et al. [32] proposed an advanced temporal credential-based security scheme with mutual authentication and key agreement for WSNs. Turkanović and Hölbl [33] claimed that Das et al.'s protocol [28] is infeasible for real-life implementation and presented an enhanced user authentication protocol based on Das et al.'s protocol [28].

In 2014, Farash et al. [34] proposed an improved three-party password based authenticated key exchange protocol using extended chaotic maps. Turkanović et al. [35] designed a novel user authentication and key agreement protocol for heterogeneous ad hoc WSNs based on the IoT notion.

In 2015, He et al. [36] proved that Xue et al.'s protocol [29] suffers from user impersonation attacks, sensor node impersonation attacks, modification attacks, and does not provide user anonymity. Hence, He et al. [36] presented a secure temporal-credential based mutual authentication and key agreement scheme with pseudo identity for WSNs. Amin and Biswas [37] proposed a protocol based on three-factor user authentication and key agreement, which is usable for telecare medical information system (TMIS). Amin et al. [38] presented a remote patient authentication protocol which preserves user anonymity and fixes the security pitfalls of Das et al.'s protocol [39]. Amin and Biswas [40] proposed three-party authenticated key exchange protocol using smart card based on the cryptographic one-way hash function. Farash et al. [41] presented a provably secure and efficient two-party password-based explicit authenticated key exchange protocol.

In 2016, Heydari et al. [42] proposed a password-based authenticated key exchange protocol for mobile networks, which has provable security. Amin and Biswas [43] presented an authentication protocol using smart card, which is based on an architecture applicable for distributed cloud environment, where a registered user can access all private information securely from all private cloud servers. Amin and Biswas [43] claimed that Turkanović et al.'s protocol [35] has some security weaknesses. Therefore, Amin and Biswas [43] addressed the vulnerabilities of Turkanović et al.'s protocol [35]. Das et al. [44] proposed an efficient multi-gateway based three-factor user authentication and key agreement protocol in hierarchical WSNs. Irshad et al. [45] proposed an anonymous multi-server authenticated key agreement based on chaotic map without engaging registration center. Heydari et al. [46] presented an improved one-to-many authentication protocol which is based on bilinear pairings.

In 2017, Mohit et al. [47] presented an authentication protocol for WSN based vehicular sensor networks. At the same year, Irshad et al. [48] proposed an improved chaotic map based authenticated key agreement for multi-server architecture to fix security vulnerabilities of Tan's protocol [49].

Recently, scholars have put forward several interesting authentication and key agreement protocols that are either two-factor or three-factor. Wu et al. [50] have proposed a lightweight two-factor scheme for healthcare applications by utilization of wireless medical sensor networks. They have taken the advantage of ProVerif for the formal security verification. Nevertheless, careful evaluation of their scheme indicates that it cannot entirely fulfil security requirements, such as perfect forward secrecy. In addition, Mishra et al. [51] have suggested an authentication scheme for multimedia communications in IoT based WSN. Although their scheme provides a high level of efficiency, such as a comparable storage cost to our presented one in this paper, like [50], it also fails to provide perfect forward secrecy or cannot resist sensor untraceability attack. There is yet another efficient authenticated key exchange scheme by Jangirala et al. [12] for industrial IoT. In [12], the authors benefit from the Chebyshev chaotic map cryptosystem, as one of the most efficient public key cryptosystem, for the key agreement. Nonetheless, as the Chebyshev cryptosystem is very slower than symmetric encryption/decryption or hash operation [52,53], their scheme needs much more computational power than the presented ones in [50, 51].

Yet another key agreement framework has been proposed recently by Fadi Al-Turjman et al. [54] by the employment of the ECC and bilinear pairing. Although their proposed scheme can properly provide resiliency against the well-known attacks, it has more computational overhead than similar schemes. To indicate the security provision of the proposed scheme, they have used the Burrows Abadi Needham (BAN) logic.

3. Weaknesses of Amin et al.'s protocol

Amin et al. [14] have claimed that their protocol could withstand several security attacks. However, this section demonstrates that their protocol is vulnerable to strong replay attacks and also does not provide perfect forward secrecy. The details are as follows.

3.1. Strong replay attacks

The synchronization of the user and GWN is difficult in authentication protocols because the user only has a smart card. In Amin et al.'s protocol [14], it has been clearly stated that the timestamp verification is done in steps 2 and 3 to provide resistance against replay attacks. The provided resistance in Amin et al.'s protocol [14] is not enough and replay attacks can still take place as follows and illustrated in Fig. 2. The adversary captures the communication channel between the user and GWN, which is a public and insecure channel, and obtains the transmitting messages MSG_1 and MSG_3. After obtaining MSG_1 and MSG_3, the adversary immediately resends the captured login request message MSG_1 to the GWN. Without logging in, even though this message comes from an expired session, it will not be rejected, resulting the GWN to compute MSG_2 and send it to user which is an adversary. The saved message MSG_3 is then sent by the adversary as a response, causing the GWN to continue the protocol by sending the message MSG_4 to the sensor node. The next step of the protocol requires that S_j computes MSG_5 and sends it to the GWN, and the GWN computes MSG_6 and sends it to the adversary. It is in this step that the adversary can authenticate itself as a legitimate user by cheating S_j and the GWN.

3.2. Lack of perfect forward secrecy

If exposing the secret long-term parameters of parties (password of the user or the secret key of the GWN) leads to jeopardizing the previously negotiated session keys, then it is said that the protocol does not provide perfect forward secrecy. This section shows that in Amin et al.'s protocol [14], exposing the master key of the GWN leads to jeopardizing the previously negotiated session keys. The details are as follows.

Step 1: By eavesdropping the messages MSG_1 and MSG_5, the adversary acquires the values of $\langle T_1, SCT_i, M_1, M_2, M_{10}\rangle$. Thus having X_{GWN} and SCN_i he/she can compute L_i.

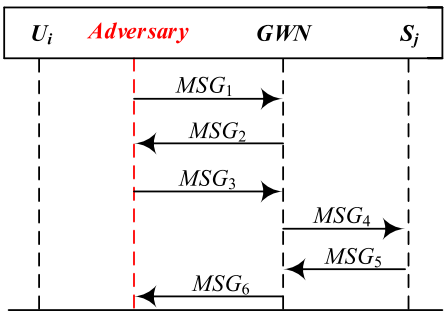

Fig. 2. Strong replay attacks in Amin et al.'s protocol.

Step 2: ID_i can be achieved as $ID_i = M_1 \oplus h(L_i \| T_1)$.

Step 3: Having X_{GWN} and ID_i, d_i is attained. By placing d_i in $K_i = M_2 \oplus h(d_i \| T_1)$, K_i is achieved.

Step 4: Having K_i, the adversary calculates $K_j = K_i \oplus M_{10}$, so K_j can be acquired.

Step 5: Finally, since ID_j is public, session key can be achieved as $SK = h(ID_i \| ID_j \| K_i \| K_j)$.

As a result, Amin et al.'s protocol [14] cannot provide perfect forward secrecy.

4. Weakness of Jiang et al.'s protocol

Jiang et al. [15] suggested a lightweight three-factor authentication and key agreement scheme for WSNs. However, we prove that Jiang et al.'s protocol also does not provide perfect forward secrecy as Amin et al.'s protocol [14]. The details are as follows.

Assuming that the adversary obtains X_j will lead to jeopardizing the previously negotiated session keys.

Step 1: The adversary obtains MSG_2 and MSG_3 by eavesdropping the communication channel, which is a public channel. Hence, the adversary can obtain $\langle T_2, T_3, M_5, M_6, M_7 \rangle$.

Step 2: With guessing ID_i and ID_j, the adversary computes $K_i^{**} = M_5 \oplus h(ID_i^{**} \| ID_j \| X_j \| T_2)$.

Step 3: Having K_i^{**}, the adversary calculates $K_j = K_i^{**} \oplus M_7$.

Step 4: Then, the adversary can compute $SK_j = h(ID_i^{**} \| ID_j \| K_i^{**} \| K_j)$ and finally to confirm the guess, puts SK_j in M_6 and checks whether SK_j is correct or not.

Thus, Jiang et al.'s protocol [15] cannot provide perfect forward secrecy.

5. The proposed protocol

In order to overcome the security weaknesses of Amin et al.'s protocol [14] and Jiang et al.'s protocol [15], a secure and efficient authentication and key agreement protocol for WSNs is proposed in this section. The proposed protocol consists of four phases: system setup phase, registration phase, login and verification phase, and password change phase. The list of notations used in the proposed protocol is given in Table 1. The details are as follows.

5.1. System setup phase

This stage is executed offline by the system administrator (SA).

Step 1. The SA selects an identity ID_j for every sensor node (S_j) and a master key X_{GWN}, which is unknown to everyone except the GWN.

Table 1
List of notations used in the proposed protocol.

Notation	Description
S_j	Sensor node
U_i	User
SA	System administrator
SCN_i	Unique smart card number
GWN	Gateway node
PW_i	Password of U_i
PW_i^{new}	New password of U_i
ID_i	Identity of U_i
ID_j	Identity of S_j
BK	Biometric key generation/extraction function
B_i	Biometric of U_i
X_{GWN}	Secret key of GWN
X_j	Secret key of S_j
K_i	Random number generated by U_i
K_j	Random number generated by S_j
r_1	Random number generated by GWN
R_{SA_i}	Random number generated by SA
R_{shrd}	Shared random number between GWN an S_j
T_i	Timestamp
SK_i	Generated session key by U_i
SK_j	Generated session key by S_j
SK_{GWN}	Generated session key by GWN
ΔT	Constant transmission delay
$h(.)$	One-way hash function
$H(.)$	Bio-hashing function
$\|$	Concatenation operation

Step 2. The GWN computes $X_j = h(ID_j \| X_{GWN})$. The X_j is the secret key and it is different for each S_j.

Step 3. The SA chooses a random number R_{shrd}, which is shared between the GWN and S_j. Eventually, the SA embeds (ID_j, X_j, R_{shrd}) into the tamper-proof memory of S_j in a secure manner. Amin et al. [14] has presumed that the adversary will not be able to extract these three parameters (ID_j, X_j, R_{shrd}).

5.2. User registration phase

This phase is illustrated in Fig. 3 and also the explanation is given below.

Step 1. The user (U_i) selects an identity ID_i and sends it to the SA via a secure channel. The secure channel can be provided for example by the physical presence of the user in the SA office. As this is done once, it is not a big deal.

Step 2. The SA checks the existence of ID_i in the database. If it exists, the SA requests another identity; otherwise, selects random number R_{SA_i} that is specific for each U_i and computes $A_i = h(ID_i \| R_{SA_i} \| X_{GWN})$ with secret key of GWN. Also, the SA generates SCN_i, which is a unique number, and computes $L_i = h(SCN_i \| X_{GWN})$. After that, the SA stores $\langle A_i, L_i, SCN_i, BK() \rangle$ into the memory of a smart card and sends it to the U_i through a secure channel. Moreover, the SA keeps a table, which stores the ID_i of each U_i. Then, the SA sends ID_i and R_{SA_i} to the GWN.

Step 3. The U_i inserts the smart card into a card reader. The U_i inputs fingerprint B_i at the sensor device and $\langle ID_i, PW_i \rangle$ in the smart card. At that moment, the smart card selects a random number RN_i. The smart card computes masked biometric $C_i = BK(H(B_i)) \oplus RN_i$, $RPW_i = h(ID_i \| PW_i \| RN_i)$, $D_i = RPW_i \oplus A_i$, $E_i = h(ID_i \| PW_i \| RN_i) \oplus Li$. Finally, the reader stores $\langle D_i, C_i, E_i, SCN_i, BK() \rangle$ into the memory and removes $\langle A_i, L_i \rangle$ from it.

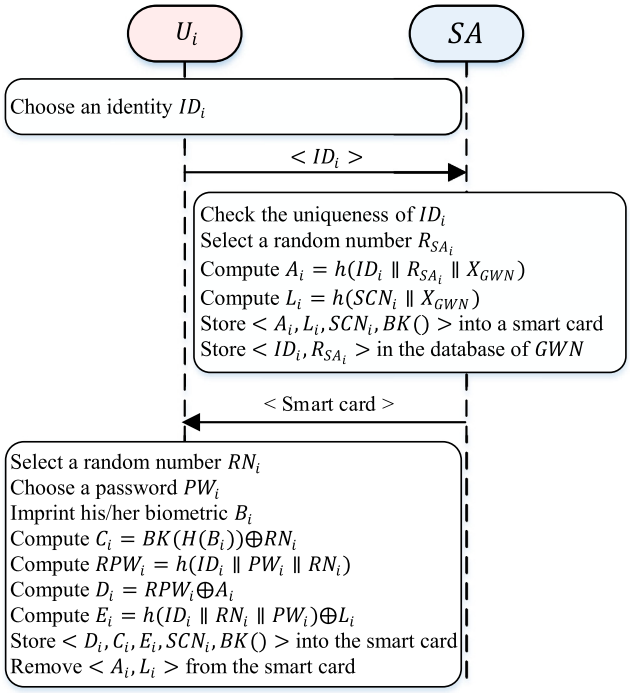

Fig. 3. User registration phase of the proposed protocol.

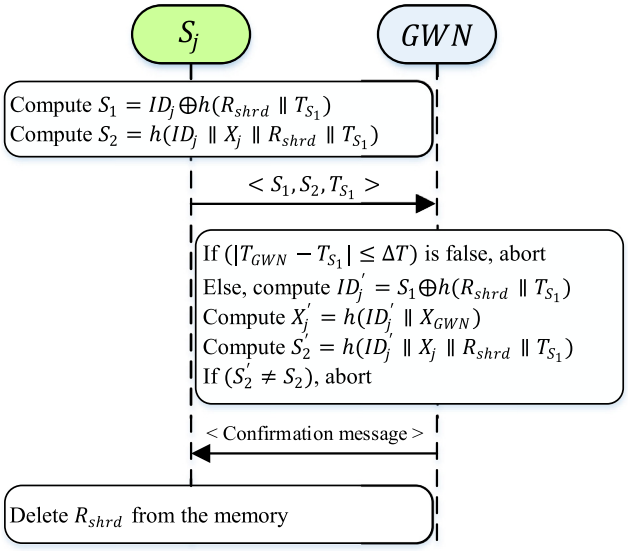

Fig. 4. Sensor node registration phase of the proposed protocol.

5.3. Sensor node registration phase

The illustration of this phase is depicted in Fig. 4 and the description is as follows. Each S_j executes the following procedure to register with the GWN.

Step 1. Having ID_j, X_j, and R_{shrd}, the S_j first computes $S_1 = ID_j \oplus h(R_{shrd} \| T_{S_1})$ and $S_2 = h(ID_j \| X_j \| R_{shrd} \| T_{S_1})$ and then sends $\langle S_1, S_2, T_{S_1} \rangle$ to the GWN through an insecure channel.

Step 2. The GWN verifies whether $|T_{GWN} - T_{S_1}| \leq \Delta T$ holds. If it is incorrect, the GWN rejects the request of the S_j; otherwise, it computes $ID_j' = S_1 \oplus h(R_{shrd} \| T_{S_1})$, $X_j' = h(ID_j' \| X_{GWN})$, $S_2' = h(ID_j' \| X_j \| R_{shrd} \| T_{S_1})$ and checks whether $S_2' = S_2$ holds. If it is incorrect, the GWN rejects this request; otherwise, authenticates the S_j and stores ID_j into the database. After that, the GWN sends a confirmation message to the S_j.

Step 3. After receiving the confirmation message, the S_j deletes R_{shrd} from its memory.

5.4. Login and authentication phase

In order for any registered U_i to access the information of S_j, this phase must be executed beforehand. The steps of this phase are done through an unreliable channel as illustrated in Fig. 5 and explained below.

Step 1. The U_i inserts his/her smart card into the smart card reader and also imprints his/her fingerprint at the related sensors. The smart card reader first extracts C_i and computes masked biometric $RN_i' = BK(H(B_i)) \oplus C_i'$; then, it checks whether $C_i' = C_i$. If the condition does not hold, it aborts the connection; otherwise, it prompts U_i to input ID_i and PW_i. Following, the smart card computes $RPW_i' = h(ID_i \| PW_i \| RN_i)$. If $RPW_i' \neq RPW_i$, U_i's login request will be rejected, else the smart card confirms that $PW_i' = PW_i$ and $ID_i' = ID_i$. After that the U_i is verified, the smart card computes $A_i' = D_i \oplus RPW_i$ and $L_i' = E_i \oplus RPW_i$. Also, the smart card generates a random number K_i and a timestamp T_1. The smart card computes $M_1 = ID_i' \oplus h(L_i' \| T_1)$, $M_2 = K_i \oplus h(A_i' \| T_1)$, $M_3 = h(A_i' \| K_i \| T_1)$, and $SCT_i = SCN_i \oplus h(T_1)$. Next, the smart card reader asks U_i for the identity of a S_j. The U_i selects a S_j and inserts its ID_j to the reader. The smart card reader computes $EID_j = ID_j \oplus h(ID_i \| K_i \| T_1)$ and submits $MSG_1 = (M_1, M_2, M_3, T_1, SCT_i, EID_j)$ to the GWN through an insecure channel.

Step 2. The GWN verifiers whether $|T_2 - T_1| \leq \Delta T$ is correct or not based on the T_2. If the verification does not hold, aborts the session; otherwise, computes $SCN_i = SCT_i \oplus h(T_1)$, $L_i' = h(SCN_i \| X_{GWN})$, and $ID_i' = M_1 \oplus h(L_i' \| T_1)$. Afterward, the GWN retrieves R_{SA_i} based on ID_i from the database and computes $A_i' = h(ID_i \| R_{SA_i} \| X_{GWN})$, $K_i' = M_2 \oplus h(A_i' \| T_1)$, and $M_3' = h(A_i' \| K_i' \| T_1)$. If $M_3' \neq M_3$, the GWN rejects the session; otherwise, chooses a random number r_1 and computes $M_4 = h(ID_i \| A_i' \| T_2 \| r_1)$ and $R_1 = r_1 \oplus h(A_i \| T_2)$. Then, the GWN sends $MSG_2 = (M_4, R_1, T_2)$ to U_i through an insecure channel.

Step 3. After getting the message, first, the U_i checks the condition $|T_3 - T_2| \leq \Delta T$ based on the current T_3. The U_i computes $r_1 = R_1 \oplus h(A_i' \| T_2)$ and $M_4' = h(ID_i \| A_i' \| T_2)$. The U_i will abort the session if $M_4' \neq M4$; otherwise, computes $M_5 = h(A_i' \| ID_i \| K_i \| r_1 \| T_3)$. Finally, U_i forwards $MSG_3 = (M_5, T_3)$ to the GWN through an insecure channel.

Step 4. The GWN verifiers whether $|T_4 - T_3| \leq \Delta T$ is correct or not based on the T_4. If the verification does not hold, aborts the session; otherwise, computes $M_5' = h(A_i' \| ID_i' \| K_i' \| r_1 \| T_3)$. If $M_5' \neq M_5$, the GWN rejects the connection; otherwise, goes to the next step. As soon as the authenticity of U_i is proved, the GWN computes $ID_j' = EID_j \oplus h(ID_i \| K_i \| T_3)$, $X_j' = h(ID_j' \| X_{GWN})$, $M_6 = h(ID_i' \| ID_j' \| ID_{GWN} \| X_j' \| K_i' \| T_4)$, $M_7 = ID_i' \oplus h(ID_{GWN} \| X_j' \| T_4)$, and $M_8 = K_i \oplus h(ID_i' \| X_j')$. Lastly, the GWN sends $MSG_4 = (ID_{GWN}, M_6, M_7, M_8, T_4)$ to the S_j through an insecure channel.

Step 5. After getting the message, the S_j checks the condition $|T_5 - T_4| \leq \Delta T$ based on the current T_5. If it is incorrect, aborts the connection; otherwise, computes $ID_i' =$

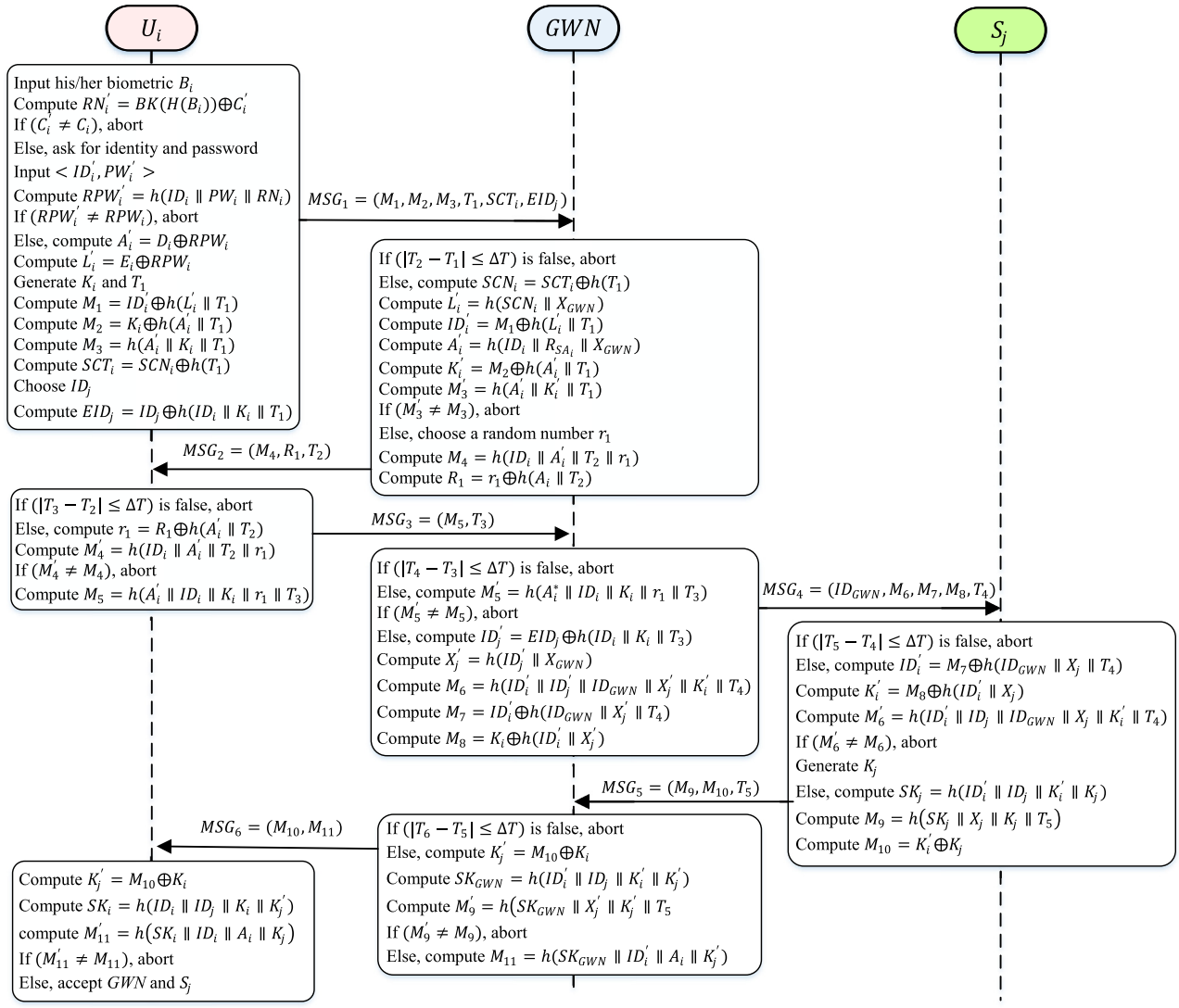

Fig. 5. Login and authentication phase of the proposed protocol.

$M_7 \oplus h(ID_{GWN} \| X_j \| T_4)$, $K_i' = M_8 \oplus h(ID_i' \| X_j)$, and $M_6' = h(ID_i' \| ID_j \| ID_{GWN} \| X_j \| K_i' \| T_4)$. If $M_6' \neq M_6$, the S_j aborts the connection; otherwise, believes that the U_i and the GWN are authentic. Moreover, the S_j generates a random number K_j and computes $SK_j = h(ID_i' \| ID_j \| K_i' \| K_j)$, $M_9 = h(SK_j \| X_j \| K_j \| T_5)$, and $M_{10} = K_i' \oplus K_j$. Ultimately, the S_j sends $MSG_5 = (M_9, M_{10}, T_5)$ to the GWN through an insecure channel.

Step 6. The GWN verifiers whether $|T_6 - T_5| \leq \Delta T$ is correct or not based on T_6. If the verification does not hold, aborts the session; otherwise, computes $K_j' = M_{10} \oplus K_i$, $SK_{GWN} = h(ID_i' \| ID_j \| K_i' \| K_j')$, and $M_9' = h(SK_{GWN} \| X_j' \| K_j' \| T_5)$. If $M_9' \neq M_9$, the GWN aborts the session; otherwise, computes $M_{11} = h(SK_{GWN} \| ID_i' \| A_i \| K_j')$. Eventually, the GWN sends $MSG_6 = (M_{10}, M_{11})$ to the U_i through an insecure channel.

Step 7. The U_i computes $K_j' = M_{10} \oplus K_i$, $SK_i = h(ID_i \| ID_j \| K_i \| K_j')$, and $M_{11}' = h(SK_i \| ID_i \| A_i \| K_j)$. If $M_{11}' \neq M_{11}$ the U_i aborts the session; otherwise, believes that the S_j and the GWN are authentic.

5.5. Password change phase

In order for an authorized U_i to be able to update the PW_i, password-based authentication protocols require a password change mechanism. In order to decrease the complexity and network congestion, the password change must be done without any help from the SA or the GWN. To do so, U_i can execute the following steps.

Step 1. U_i inserts the smart card into the card reader and executes step 1 of the login and authentication phase to verify the validity of fingerprint, password, and identity.

Step 2. The smart card reader requests a new password PW_i^{new} from U_i. Then U_i enters a new password PW_i^{new}. The smart card computes $RPW_i^{new} = h(ID_i \| PW_i^{new} \| RN_i)$, $A_i' = D_i \oplus RPW_i$, $D_i^{new} = A_i^{new} \oplus RPW_i$, $L_i' = E_i \oplus RPW_i$, and $E_i^{new} = L_i' \oplus RPW_i$.

Step 3. The smart card reader updates $\langle D_i, E_i \rangle$ with $\langle D_i^{new}, E_i^{new} \rangle$.

6. Security correctness with AVISPA

In this section, the security of the proposed authentication protocol is analyzed. For this purpose, we have simulated the authentication protocol using the widely-accepted AVISPA software. The AVISPA simulation tool determines whether the proposed security protocol is SAFE or UNSAFE and verifies the security correctness in this way [55]. High Level Protocol Specification Language (HLPSL) is supported by this software along with four

```
% OFMC
% Version of 2006/02/13
SUMMARY
    SAFE
DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
   /cdrom/avispa-1.1/testsuite/results/WSN.if
GOAL
   as_specified
BACKEND
   OFMC
COMMENTS
STATISTICS
   prseTime: 0.00s
   searchTime: 0.34s
   visitedNodes: 158 nodes
   depth: 6 plies
```

Fig. 6. The results of analyzing the proposed protocol using the AVISPA tool.

different back-ends and abstraction based methods, which are integrated with HLPSL. When an authentication protocol is reported as SAFE by the AVISPA under the on the fly model checker (OFMC) and the back-end constraint logic based attack searcher (CL-AtSe), it means that the protocol is secure against active and passive attacks [56]. The results of analyzing the proposed protocol using the AVISPA (OFMC back-end) are shown in Fig. 6. As the results show, the proposed protocol is secure against active and passive attacks.

7. Further security analysis

The informal security analysis of the proposed protocol against various attacks is presented in this section.

7.1. Secure against offline user identity guessing attacks

(1) In the proposed protocol, the adversary cannot derive or guess ID_i from the smart card information. We assume that the adversary has intercepted the login message $\langle M_1, M_2, M_3, T_1, SCT_i, EID_j\rangle$. Since the secret key of the GWN is in L_i, ID_i cannot be derived from M_1. It is also not possible to derive ID_i from EID_j because it is protected by the one-way hash function.

(2) While executing step 1 and step 2, M_4 and M_5 are exchanged between the GWN and U_i. Since M_4 and M_5 are protected by the one-way hash function, the adversary cannot guess or extract ID_i using them.

Therefore, the proposed protocol can resist against offline user identity guessing attacks.

7.2. Secure against offline sensor identity guessing attacks

(1) We assume that the adversary can intercept the channel and achieve EID_j. However, K_i and ID_i are also required to derive ID_j, which is not possible.

(2) Assume that the adversary intercepted message MSG_4. Since ID_j is protected by the hash function in M_6, the adversary cannot guess it.

Hence, the proposed protocol can resist against offline sensor identity guessing attacks.

7.3. Secure against offline password guessing attacks

Assume that the adversary steals or finds a user's smart card and retrieves $\langle D_i, C_i, E_i, SCN_i, BK()\rangle$ from the memory of the smart card. The adversary can only guess the pair $(ID_i \| PW_i)$ and cannot guess PW_i. Likewise, because the user chooses a random number RN_i and uses it in E_i and C_i, the adversary can compute neither E_i nor C_i. Therefore, the proposed protocol can withstand the offline password guessing attacks.

7.4. Secure against replay attacks

Suppose that the adversary eavesdrops MSG_1 and MSG_2 from the authentication phase through an insecure channel. Next time, the adversary may intend to use this message but because the GWN chooses a random number and generates $R_1 = r_1 \oplus h(A_i \| T_2)$ and sends it with M_4 to the user, he/she cannot use this message to continue the protocol. Hence, the proposed protocol can resist the replay attacks.

7.5. Perfect forward secrecy

In the proposed protocol, $SK = h(ID_i \| ID_j \| K_i \| K_j)$ is a shared session key between the user, sensor node, and the gateway node. Even if an adversary obtains the secret key of the gateway node X_{GWN} or the user's password, PW_i, he/she is still not able to compute old session keys. Because the SA generates a new random number R_{SA_i} for any user, the adversary cannot compute the session key. Therefore, the perfect forward secrecy is supported in the proposed protocol.

7.6. User anonymity

In the proposed protocol, the ID_i is never transmitted over the insecure channel. If the adversary gets the user's login request message $\langle M_1, M_2, M_3, T_1, SCT_i, EID_j\rangle$, he/she cannot reveal the ID_i, because it is hashed. Hence, it is impossible for the adversary to reveal the ID_i from the login and authentication messages. So the user's anonymity is provided in the proposed protocol.

7.7. Impersonation attacks

The adversary cannot produce a legal login request message $\langle M_1, M_2, M_3, T_1, SCT_i, EID_j\rangle$, because he/she does not know the L_i, A_i, K_i, and ID_i. The adversary may steal a smart card and retrieve $\langle A_i, L_i\rangle$ from the memory of the smart card, where $A_i = h(ID_i \| R_{SA_i} \| X_{GWN})$ and $L_i = h(SCN_i \| X_{GWN})$. Because the adversary does not know $\langle R_{SA_i}, X_{GWN}\rangle$, he/she cannot impersonate a legal user.

8. Performance analysis

In this section, the proposed protocol of this paper and other related protocols are evaluated and compared based on features such as cost of storage, communication, and computation. The results of this evaluation are reported in the following tables to show the effectiveness and efficiency of the suggested protocol.

Table 2
Comparison of the proposed protocol with other related ones.

Protocol	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8
Yeh et al. [17]	No	No	No	Yes	No	No	No	No
Das et al. [28]	No	No	No	No	No	Yes	No	No
Xue et al. [29]	No	No	No	No	No	No	No	No
Turkanović and Hölbl [33]	No	No	No	Yes	No	Yes	No	No
Turkanović et al. [35]	No	No	No	No	Yes	No	No	No
Amin and Biswas [43]	No	Yes	Yes	No	Yes	Yes	Yes	Yes
Mishra et al. [51]	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Wu et al. [50]	Yes	Yes	No	No	No	No	No	Yes
Amin et al. [14]	Yes	Yes	Yes	No	No	No	Yes	Yes
Jiang et al. [15]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

R_1: Resist user identity guessing attacks; R_2: Resist sensor identity guessing attacks; R_3: Resist user and sensor untraceability attacks; R_4: Resist password guessing attacks; R_5: Resist replay attacks; R_6: Perfect forward secrecy; R_7: Resist user anonymity; R_8: Resist impersonation attacks. Yes: The protocol can resist the attacks; No: The protocol is vulnerable to the attacks.

8.1. Security and functionality comparison

For the purpose of comparing the proposed protocol with other protocols, a number of security attacks and functionality requirements are shown in Table 2. As seen in Table 2, the protocols in [14,28,29,35,43,50] are vulnerable to the offline password guessing attacks and the protocols in [27–29,33,35] cannot achieve safety against offline user and sensor identity guessing attacks. We have also found the protocols in [14,17,28,29,33,50] suffer from the replay attacks.

Furthermore, the protocols in [14,15,17,29,35,51,50] do not provide perfect forward secrecy. Hence, the proposed protocol is more suitable than the previous protocols.

8.2. Computational cost comparison

In WSNs, energy is an important factor and design limiting option in employing security algorithms. Therefore, the user authentication protocol should not require heavy computations. The proposed protocol uses the hash function instead of other costly operations, such as public key cryptographic operations, because the hash function is much more lightweight than operations like asymmetric encryption/decryption. The reported results in [57] show that the running time of a symmetric key encryption/decryption function is $T_{e/d} \approx 0.1303$ ms and the running time of a hash function is $T_h \approx 0.0004$ ms. In addition, modular squaring is similar to hash function and the computation time of a square module N is the same as encryption. The computations and running time of the proposed protocol and the presented ones in [14,15,17,28,29,33,35,43,51,50] for U_i, GWN, and S_j are presented in Table 3 and Fig. 7.

In the proposed protocol, the number of T_h for U_i, GWN, and S_j are 11, 17, and 5, respectively. Hence, the total computational cost of the suggested protocol is $11T_h+5T_h+17T_h = 33T_h$ and the running time is $33T_h \times 0.0004 = 0.0132$ ms. Although the computational cost of the proposed protocol is slightly more than the presented ones in [35,43,51], according to Table 2, the proposed protocol is safe to various attacks. Protocol [35] is vulnerable to the offline user identity guessing attacks, offline sensor identity guessing attacks, user and sensor untraceability guessing attacks, offline password guessing attacks, and impersonation attacks and does not provide perfect forward secrecy and user anonymity. Also, protocol [43] is vulnerable to the offline user identity guessing attacks and replay attacks. Likewise, protocol [51] does not support perfect forward secrecy. In addition, despite the fact that protocol [14] has the same computational cost, it is vulnerable to well-known attacks that the proposed protocol is resistant against them. Protocol [15] also does not provide perfect forward secrecy.

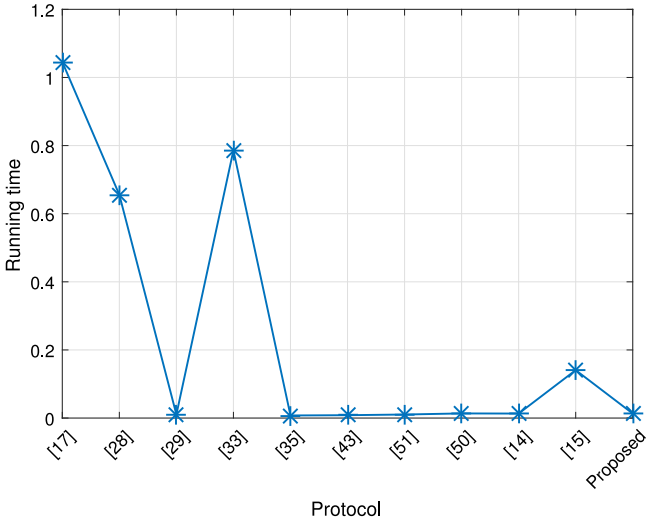

Fig. 7. Comparative running time.

8.3. Communication cost comparison

The communication cost of a protocol must be as low as possible in order to provide low network congestion and quick message transmission. The output of hash function, random number, timestamp, and user identity is 128 bits.

In the proposed protocol, U_i transmits $MSG_1 = (M_1, M_2, M_3, T_1, SCT_i, EID_j)$ and $MSG_3 = (M_5, T_3)$ and receives $MSG_2 = (M_4, R_1, T_2)$ and $MSG_6 = (M_{10}, M_{11})$. Thus, the communication cost for the U_i is $13 \times 128 = 1664$. S_j transmits $MSG_5 = (M_9, M_{10}, T_5)$ and receives $MSG_4 = (ID_{GWN}, M_6, M_7, M_8, T_4)$, so the communication cost for the S_j is $8 \times 128 = 1024$. The GWN transmits $MSG2 = (M_4, R_1, T_2)$, $MSG_4 = (ID_{GWN}, M_6, M_7, M_8, T_4)$, and $MSG_6 = (M_{10}, M_{11})$ and receives $MSG_1 = (M_1, M_2, M_3, T_1, SCT_i, EID_j)$, $MSG_3 = (M_5, T_3)$, and $MSG_5 = (M_9, M_{10}, T_5)$. Therefore, the communication cost for the GWN is $21 \times 128 = 2688$. In conclusion, in the proposed protocol, the total cost is $1664 + 1024 + 2688 = 5376$ bits. The communication cost of the other schemes is presented in Table 4 and Fig. 8. Although the communication cost of the proposed protocol is more than some others, in terms of security, it is resistant to various attacks.

8.4. Storage cost comparison

The total number of the cluster heads of the presented protocols in [14,15,17,28,29,33,35,43,51,50] is shown through CH^* in Table 5 and Fig. 9. It is worth mentioning that the cluster heads

Table 3
Comparison of the running time of the proposed protocol with other related ones.

Protocol	U_i	S_j	GWN	Total computation	Running time
Yeh et al. [17]	$1T_h + 2T_{(d/e)}$	$3T_h + 2T_{(d/e)}$	$4T_h + 4T_{(d/e)}$	$8T_h + 8T_{(d/e)}$	1.0456 ms
Das et al. [28]	$5T_h + 1T_{(d/e)}$	–	$5T_h + 4T_{(d/e)}$	$10T_h + 5T_{(d/e)}$	0.6555 ms
Xue et al. [29]	$7T_h$	$6T_h$	$13T_h$	$26T_h$	0.0104 ms
Turkanović and Hölbl [33]	$4T_h + 1T_{(d/e)}$	–	$7T_h + 5T_{(d/e)}$	$11T_h + 6T_{(d/e)}$	0.7862 ms
Turkanović et al. [35]	$7T_h$	$5T_h$	$7T_h$	$19T_h$	0.0076 ms
Amin and Biswas [43]	$8T_h$	$5T_h$	$8T_h$	$21T_h$	0.0084 ms
Mishra et al. [51]	$9T_h$	$6T_h$	$11T_h$	$26T_h$	0.0104 ms
Wu et al. [50]	$11T_h$	$6T_h$	$17T_h$	$34T_h$	0.0136 ms
Amin et al. [14]	$12T_h$	$5T_h$	$16T_h$	$33T_h$	0.0132 ms
Jiang et al. [15]	$8T_h + 1T_M$	$5T_h$	$12T_h + 1T_{QR}$	$25T_h + 1T_M + 1T_{QR}$	0.1407 ms
Proposed	$11T_h$	$5T_h$	$17T_h$	$33T_h$	0.0132 ms

Table 4
Communication cost comparison of the proposed protocol with other related ones.

Protocol	U_i	S_j	GWN	Total communication
Yeh et al. [17]	896	3200	896	4992
Das et al. [28]	768	0	768	1536
Xue et al. [29]	1280	1152	1920	4352
Turkanović and Hölbl [33]	768	0	768	1536
Turkanović et al. [35]	1408	3200	1772	6380
Amin and Biswas [43]	1408	1280	2432	5120
Mishra et al. [51]	1280	1152	2432	4864
Wu et al. [50]	1408	768	2176	4352
Amin et al. [14]	1280	1024	2304	4608
Jiang et al. [15]	768	1024	1792	3584
Proposed	1664	1024	2688	5376

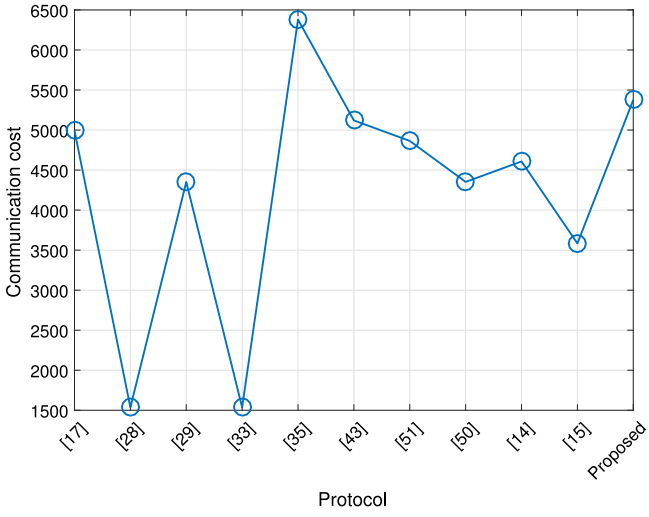

Fig. 8. Comparative communication cost.

Table 5
Storage cost comparison of the proposed protocol with other related ones.

Protocol	Storage cost
Yeh et al. [17]	896
Das et al. [28]	$768 + CH^*$
Xue et al. [29]	640
Turkanović and Hölbl [33]	$768 + CH^*$
Turkanović et al. [35]	768
Amin and Biswas [43]	640
Mishra et al. [51]	512
Wu et al. [50]	640
Amin et al. [14]	640
Jiang et al. [15]	896
Proposed	512

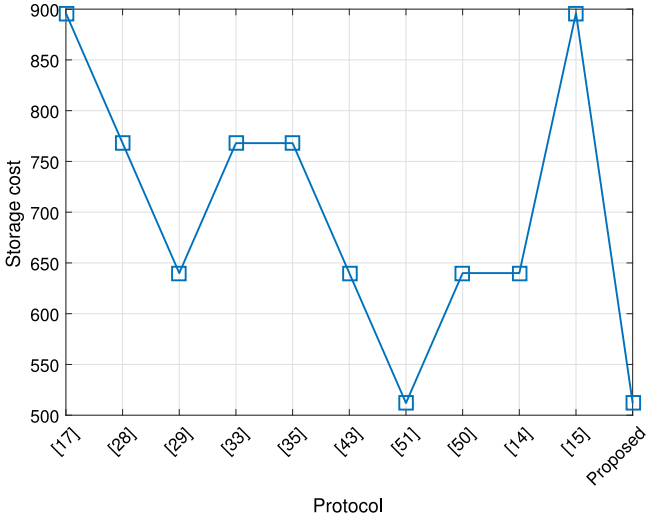

Fig. 9. Comparative storage cost.

collect the data from the respective cluster nodes and forward the aggregated data to base station.

The length of the identity, password, random number, and hash output is considered to be 128 bits. In the proposed protocol, for each user, we store $\langle D_i, C_i, E_i, SCN_i \rangle$ in the smart card. As a result, the storage cost of the proposed scheme is $128 + 128 + 128 + 128 = 512$ bits. We found that the smart card storage cost of the protocols in [28,33] is more than the storage cost of the other protocols. This is because the protocols in [28,33] store the key of every cluster head into the smart card.

9. Conclusion

In this article, we have done the cryptanalysis of Amin et al.'s protocol and have found its security vulnerabilities, such as strong replay attacks and lack of perfect forward secrecy. Likewise, we have proved that Jiang et al.'s scheme does not provide perfect forward secrecy as Amin et al.'s protocol. Therefore, according to

Amin et al.'s protocol, we have presented a three-factor authentication and key agreement protocol for IoT based WSN, which is both lightweight and is free from the security flaws of previous protocols with reduced saved parameters in smart card. To verify the security, we have simulated the proposed protocol with the AVISPA tool reporting that the proposed protocol is secure against active and passive attacks. Further, the comparative efficiency analysis indicates that the proposed protocol is appropriate and efficient for IoT based WSN environments.

Since in an IoT environment, and especially industrial IoT environment, the sensor nodes or machines should be able to communicate with each other without any user intervention, in our future work, we intend to devise a machine to machine security protocol that could fulfil the required security metrics and desired efficiency simultaneously. Although there are some efficient recently-published schemes that have addressed this topic, careful consideration of them demonstrates that they cannot totally assuage the desired security requirements.

Conflict of interest statement

None.

Declaration of competing interest

The authors declared that they had no conflicts of interest with respect to their authorship or the publication of this article.

References

[1] A.H. Mohajerzadeh, H. Jahedinia, Z. Izadi-Ghodousi, D. Abbasinezhad-Mood, M. Salehi, Efficient target tracking in directional sensor networks with selective target area's coverage, Telecommun. Syst. 68 (1) (2018) 47–65.

[2] S.A. Chaudhry, H. Naqvi, M.S. Farash, T. Shon, M. Sher, An improved and robust biometrics-based three factor authentication scheme for multiserver environments, J. Supercomput. 74 (8) (2018) 3504–3520.

[3] M. Nikooghadam, R. Jahantigh, H. Arshad, A lightweight authentication and key agreement protocol preserving user anonymity, Multimedia Tools Appl. 76 (11) (2017) 13401–13423.

[4] D. Zhang, Y. Qian, J. Wan, S. Zhao, An efficient RFID search protocol based on clouds, Mob. Netw. Appl. 20 (3) (2015) 356–362.

[5] B. Gupta, D.P. Agrawal, S. Yamaguchi, Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI global, 2016.

[6] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. 78 (2018) 964–975.

[7] M.S. Hossain, G. Muhammad, W. Abdul, B. Song, B. Gupta, Cloud-assisted secure video transmission and sharing framework for smart cities, Future Gener. Comput. Syst. 83 (2018) 596–606.

[8] A.P. Plageras, K.E. Psannis, C. Stergiou, H. Wang, B.B. Gupta, Efficient IoT-based sensor big data collection–processing and analysis in smart buildings, Future Gener. Comput. Syst. 82 (2018) 349–357.

[9] V. Adat, B. Gupta, Security in Internet of Things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. 67 (3) (2018) 423–441.

[10] S.A. Alabady, F. Al-Turjman, S. Din, A novel security model for cooperative virtual networks in the IoT era, Int. J. Parallel Program. (2018) 1–16.

[11] F. Al-Turjman, S. Alturjman, Confidential smart-sensing framework in the IoT era, J. Supercomput. 74 (10) (2018) 5187–5198.

[12] J. Srinivas, A.K. Das, M. Wazid, N. Kumar, Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things, IEEE Trans. Dependable Secure Comput. (2018).

[13] D. Abbasinezhad-Mood, M. Nikooghadam, An anonymous ECC-based self-certified key distribution scheme for the smart grid, IEEE Trans. Ind. Electron. 65 (10) (2018) 7996–8004.

[14] R. Amin, S.H. Islam, G. Biswas, M.K. Khan, L. Leng, N. Kumar, Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Comput. Netw. 101 (2016) 42–62.

[15] Q. Jiang, S. Zeadally, J. Ma, D. He, Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks, IEEE Access 5 (2017) 3376–3392.

[16] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, P. Kruus, TinyPK: securing sensor networks with public key technology, in: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM, 2004, pp. 59–64.

[17] S.H. Islam, G. Biswas, A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, J. Syst. Softw. 84 (11) (2011) 1892–1898.

[18] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.

[19] K.H. Wong, Y. Zheng, J. Cao, S. Wang, A dynamic user authentication scheme for wireless sensor networks, in: IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, SUTC'06, vol. 1, IEEE, 2006, pp. 8–pp.

[20] J. Xu, W.-T. Zhu, D.-G. Feng, An improved smart card based password authentication scheme with provable security, Comput. Stand. Interfaces 31 (4) (2009) 723–728.

[21] R. Song, Advanced smart card based password authentication protocol, Comput. Stand. Interfaces 32 (5–6) (2010) 321–325.

[22] B. Vaidya, J. Sá Silva, J.J. Rodrigues, Robust dynamic user authentication scheme for wireless sensor networks, in: Proceedings of the 5th ACM Symposium on QoS and Security for Wireless and Mobile Networks, ACM, 2009, pp. 88–91.

[23] M.L. Das, Two-factor user authentication in wireless sensor networks, IEEE Trans. Wirel. Commun. 8 (3) (2009) 1086–1090.

[24] D. He, Y. Gao, S. Chan, C. Chen, J. Bu, An enhanced two-factor user authentication scheme in wireless sensor networks, Ad Hoc Sens. Wirel. Netw. 10 (4) (2010) 361–371.

[25] R. Fan, L.-D. Ping, J.-Q. Fu, X.-Z. Pan, A secure and efficient user authentication protocol for two-tiered wireless sensor networks, in: 2010 Second Pacific-Asia Conference on Circuits, Communications and System, vol. 1, IEEE, 2010, pp. 425–428.

[26] J. Yuan, C. Jiang, Z. Jiang, A biometric-based user authentication for wireless sensor networks, Wuhan Univ. J. Nat. Sci. 15 (3) (2010) 272–276.

[27] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, H.-W. Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 11 (5) (2011) 4767–4779.

[28] A.K. Das, P. Sharma, S. Chatterjee, J.K. Sing, A dynamic password-based user authentication scheme for hierarchical wireless sensor networks, J. Netw. Comput. Appl. 35 (5) (2012) 1646–1656.

[29] K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, J. Netw. Comput. Appl. 36 (1) (2013) 316–323.

[30] M.S. Farash, M.A. Attari, R.E. Atani, M. Jami, A new efficient authenticated multiple-key exchange protocol from bilinear pairings, Comput. Electr. Eng. 39 (2) (2013) 530–541.

[31] Q. Cheng, C. Ma, Analysis and improvement of an authenticated multiple key exchange protocol, Comput. Electr. Eng. 37 (2) (2011) 187–190.

[32] C.-T. Li, C.-Y. Weng, C.-C. Lee, An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks, Sensors 13 (8) (2013) 9589–9603.

[33] M. Turkanovic, M. Holbl, An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks, Elektronika ir Elektrotechnika 19 (6) (2013) 109–117.

[34] M.S. Farash, M.A. Attari, S. Kumari, Cryptanalysis and improvement of a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, Int. J. Commun. Syst. 30 (1) (2017) e2912.

[35] M. Turkanović, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Netw. 20 (2014) 96–112.

[36] 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 (2015) 263–277.

[37] R. Amin, G. Biswas, A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity, J. Med. Syst. 39 (8) (2015) 78.

[38] R. Amin, S.H. Islam, G. 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) 140.

[39] A.K. Das, A. Goswami, A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care, J. Med. Syst. 37 (3) (2013) 9948.

[40] R. Amin, G. Biswas, Cryptanalysis and design of a three-party authenticated key exchange protocol using smart card, Arab. J. Sci. Eng. 40 (11) (2015) 3135–3149.

[41] M.S. Farash, S.H. Islam, M.S. Obaidat, A provably secure and efficient two-party password-based explicit authenticated key exchange protocol resistance to password guessing attacks, Concurr. Comput.: Pract. Exper. 27 (17) (2015) 4897–4913.

[42] M. Heydari, S.M.S. Sadough, M.S. Farash, S.A. Chaudhry, K. Mahmood, An efficient password-based authenticated key exchange protocol with provable security for mobile client–client networks, Wirel. Pers. Commun. 88 (2) (2016) 337–356.

[43] R. Amin, G. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Netw. 36 (2016) 58–80.
[44] A.K. Das, A.K. Sutrala, S. Kumari, V. Odelu, M. Wazid, X. Li, An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks, Secur. Commun. Netw. 9 (13) (2016) 2070–2092.
[45] A. Irshad, M. Sher, S.A. Chaudhary, H. Naqvi, M.S. Farash, An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging registration centre, J. Supercomput. 72 (4) (2016) 1623–1644.
[46] M. Heydari, S.M.S. Sadough, S.A. Chaudhry, M.S. Farash, K. Mahmood, An improved one-to-many authentication scheme based on bilinear pairings with provable security for mobile pay-TV systems, Multimedia Tools Appl. 76 (12) (2017) 14225–14245.
[47] P. Mohit, R. Amin, G. Biswas, Design of authentication protocol for wireless sensor network-based smart vehicular system, Veh. Commun. 9 (2017) 64–71.
[48] A. Irshad, M. Sher, M.U. Ashraf, B.A. Alzahrani, F. Wu, Q. Xie, S. Kumari, An improved and secure chaotic-map based multi-server authentication protocol based on Lu et al. and Tsai and Lo's scheme, Wirel. Pers. Commun. 95 (3) (2017) 3185–3208.
[49] Z. Tan, A privacy-preserving multi-server authenticated key-agreement scheme based on Chebyshev chaotic maps, Secur. Commun. Netw. 9 (11) (2016) 1384–1397.
[50] F. Wu, X. Li, A.K. Sangaiah, L. Xu, S. Kumari, L. Wu, J. Shen, A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks, Future Gener. Comput. Syst. 82 (2018) 727–737.
[51] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S.H. Islam, P. Gope, Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks, Multimedia Tools Appl. 77 (14) (2018) 18295–18325.
[52] A. Ostad-Sharif, A. Babamohammadi, D. Abbasinezhad-Mood, M. Nikooghadam, Efficient privacy-preserving authentication scheme for roaming consumer in global mobility networks, Int. J. Commun. Syst. (2019) e3904.
[53] D. Abbasinezhad-Mood, M. Nikooghadam, Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps, IEEE Trans. Ind. Inf. 14 (11) (2018) 4815–4828.
[54] F. Al-Turjman, Y.K. Ever, E. Ever, H.X. Nguyen, D.B. David, Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks, IEEE Access 5 (2017) 24617–24631.
[55] Y. Chevalier, L. Compagna, J. Cuellar, P.H. Drielsma, J. Mantovani, S. Mödersheim, L. Vigneron, A high level protocol specification language for industrial security-sensitive protocols, in: Workshop on Specification and Automated Processing of Security Requirements-SAPS'2004, Austrian Computer Society, 2004, pp. 13–p.
[56] D. Basin, S. Mödersheim, L. Vigano, OFMC: A symbolic model checker for security protocols, Int. J. Inf. Secur. 4 (3) (2005) 181–208.
[57] 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) 10.

Arezou Ostad-Sharif received the B.Sc. degree in Information Technology from Safahan University, Esfahan, Iran, in 2015 and M.Sc. degree in Information Security from Imam Reza International University, Mashhad, Iran, in 2017. Her M.Sc. thesis was elected as the top thesis in 2018. Her research interest is on the security protocols for Wireless Sensor Networks, Internet of Things, Smart Grids, and Telecare Medical Information Systems.

Hamed Arshad is with the Department of Informatics, University of Oslo, Norway. His research interest includes information security, network security, and cryptography.

Morteza Nikooghadam received the B.Sc. degree from university of Sajad, Iran, in 2006, M.Sc. from the Shahid Beheshti University, Iran, in 2008, and Ph.D. from Shahid Beheshti University, Iran, in 2012. He is currently an assistant professor in the Department of Computer Engineering and Information Technology at Imam Reza International University, Mashhad, Iran. His research focuses on Data Security, Cryptography, and Sensor Network Security. His current research interests are Reconfigurable Architectures for multipliers under Galois Field $GF\ (2^m)$.

Dariush Abbasinezhad-Mood received the B.Sc. degree in Computer Science from Payame Noor University, Mashhad, Iran, in 2009 and the M.Sc. degree in Secure Communications from Imam Reza International University, Mashhad, Iran, in 2016 with the first rank. Further, his M.Sc. thesis was elected as the top thesis. His research interests include Cryptography, Authentication Protocols, Smart Grid, Wireless Sensor Networks, Internet of Things, and Embedded Systems. He is a reviewer for several well-known journals, such as IEEE Transactions on Smart Grid, IEEE Transactions on Industrial Informatics, IEEE Internet of Things Journal, and IEEE Systems Journal.