IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 20, 2020, accepted April 8, 2020, date of publication April 13, 2020, date of current version April 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987764

An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network

MOSTAFA FARHADI MOGHADAM[1], MAHDI NIKOOGHADAM[2], MAYTHAM AZHAR BAQER AL JABBAN[2], MOHAMMAD ALISHAHI[3], LEILI MORTAZAVI[4], AND AMIRHOSSEIN MOHAJERZADEH[2]

[1]Khorasan Electric Distribution Company (KEDC)
[2]Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad 9177948974, Iran
[3]Department of Computer Engineering, Fariman campus, Mashhad branch, Islamic Azad University, Mashhad 9133736351, Iran
[4]Department of Computer Engineering, Khorasan Institute of Higher Education, Mashhad 9189893661, Iran

Corresponding author: Amirhossein Mohajerzadeh (mohajerzadeh@um.ac.ir)

ABSTRACT Wireless sensor networks (WSN) consist of a large number of resource-constrained sensor nodes, different types of controls, and gateway nodes. these kinds of networks are used as control systems and remote monitoring in industries such as health care, defense, agriculture, and disaster management. Due to the widespread use of wireless sensor networks, valuable information is exchanged between network entities such as sensors, gates, users, etc. in an unsafe channel, and the presence of important and sensitive information in the network increases the importance of security issues. In this article, we analyzed Majid Alotaibi schema and identify some security breaches in this article. We have also described a security attack against the proposed protocol based on security problems. In addition, to address the security issues of M. Alotaibi proposed protocol, we have introduced a mutual authentication and key agreement protocol based on ECDH (elliptic-curve Diffie–Hellman). We have implemented our own method using the Scyther tool, manually reviewed its security features and also compared it with other methods.

INDEX TERMS Authentication, wireless sensor networks, key agreement, ECDH, security, privacy.

I. INTRODUCTION

Wireless Sensor Networks (WSN) is one of the emerging technologies of the century and is becoming an epidemic technology [1]. A variety of advances have been made in the field of wireless communication and electronic science that enable the development of low-power, low-cost and performance sensor nodes. These sensor nodes, including sensor components, data processing, and communications, allow the deployment of wireless sensor networks. The wireless sensor network consists of a large number of sensor nodes that are randomly deployed to connect through the wireless environment to monitor physical or environmental conditions such as noise, vibration, pressure, temperature, etc. Co-operative transfer to the base station. In addition, the WSN has a wide variety of applications, including agriculture, industry, health care, incident management, safety monitoring, internal, surveillance systems and nuclear power plants [3]–[5]. The location of these sensors is not necessarily predetermined. In some cases, sensors are randomly distributed in hazardous or inaccessible environments [2]. Due to its rapid development, it is used in a variety of areas such as the military, home monitoring, health care, agriculture and so on. The WSN consists of the following three elements: (1) interface (2) gateway node (GW) (3) sensor node (SN). Provides a user interface for accessing GW and SN. GW enables the communication between the U user and the SN sensor node, and the SN measures the physical environment.

Sensor nodes are capable of computing and limited storage space. They collect valuable information and send it through the bus. Users can access the data collected through the gateway. Since data is transmitted through an unsecured and unprotected channel, the transmitted data must be protected against threats such as unauthorized access, illegal eavesdropping and tampering with effective action. In the future, the sensor network will be ubiquitous to make future technologies or the environment or infrastructure more intelligent. These include health care, smart homes through sensors,

The associate editor coordinating the review of this manuscript and approving it for publication was Tie Qiu.

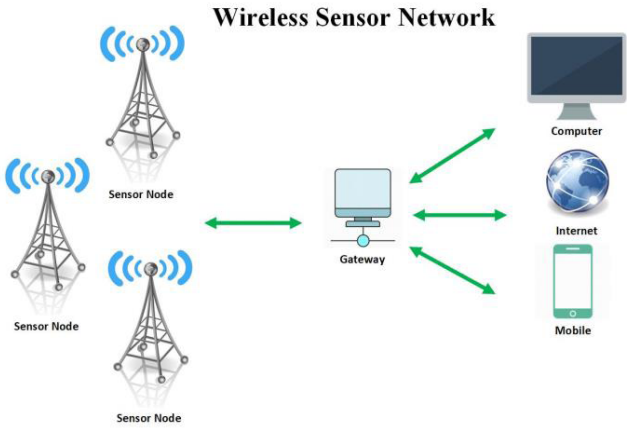


FIGURE 1. Data communication in a WSN through gateway.

environmental monitoring, and more. Figure 1 illustrate the data communication in a WSN through gateway.

Privacy, message integrity, and user authentication in such environments are crucial because enemy communications can be intercepted, deleted, or redirected [6]. Consequently, appropriate security solutions should be used to protect communication links [7].

In wireless sensor structure because of resource limitation constructions, it bears several security threats, such as hardware manipulation, eavesdropping, injecting false messages, etc., hence more efficient security mechanisms that conform to specific WSN features, are transmitted to the network. The most common security mechanism that can provide security features is symmetric cryptography [9], [10]. In such security mechanisms, when two nodes want to communicate with each other, they use a common key for the encryption and decryption process. This symmetric key has already been selected and shared by the nodes to provide message security and authentication. The process of generating shared symmetric keys is called key management [11], [12]. There is some evidence that the same symmetric keys for different sessions put nodes at risk in unsupervised and protected environments [13], [14]–[43]. Although there are systems for managing and restoring network nodes, there are still attacks that need to be identified and used to counter them [15]–[17].

A. BASIC CONCEPT

1) ELLIPTICAL CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography is a type of public key asymmetric cryptography. An elliptic curve E is a set of points to the coordinates of $pf \in *pf \in 0x, y$ which is determined by the following equations.

$$Y^2 = x^3 + ax + b$$

where $a, b \in f_p$ and $4a^3 + 27b^2 \neq 0$

The two basic operations of an elliptic curve are point sums and point multipliers, also called scalar multipliers. The following is an example of a scalar multiplication (with K times P).

$$KP = P + P + P + P \ldots . + P$$

2) DISCRETE LOGARITHM PROBLEM OR ECDLP ELLIPTIC CURVE HARD PROBLEM

Suppose P and Q are two points on the elliptic curve whose point Q is obtained by scalar multiplication of parameter k at point P. The discrete logarithm problem states that if we have two points P and Q, it is possible or even impossible to obtain the parameter k, which is known as (ECDLP) or the elliptic curve hard problem [19].

3) THE DELPHI-HELMAN ECDH ELLIPTIC CURVE

Suppose two points *p*. ai and *p*. *b*i lies on the elliptic curve. The Delphi-Hellman Curve Problem (ECDH) states that if an attacker has these two points, it is not possible to reach the points bi (ai.p) and ai (bi.p) [18], [19].

B. CONTRIBUTION

The contributions of our work are summarized as below.

- The authentication and key exchange scheme of MAJID ALOTAIB was analyzed and security problems presented.
- Due to the security weaknesses of protocol, a new schema proposed to address those security problems.
- The security analysis of the protocols has been presented and their security challenges have been represented.

A comparative analysis of the proposed protocol's performance, computational cost, formal and informal analysis is presented.

C. ORGANIZATION OF THE PAPER

After a brief review of related works in the field of wireless sensor network security, Section of the paper is as follows: we show the drawbacks and security issues of MAJID ALOTAIB protocol in Section III. The proposed protocol is presented in Section IV. The results of the security simulation of the proposed protocol using the Scyther validation tool are given in Section V, which shows the safety of the proposed protocol against several attacks. Further security analysis is provided in Section VI and the performance analysis is presented in Section VII. Finally, the conclusions of the present article are presented in Section VIII.

II. RELATED WORK

This section describes various authentication and key agreement schemes for wireless sensor network security. Over the years, many researchers have proposed schemes to enhance the security of wireless sensor networks. The key management plans and techniques that are presented in wireless sensor networks are as follows. In 2009, for securing sensor networks Wong *et al.* [20] proposed a dynamic authentication scheme that used the hash function. In the same year, another scheme base on two-factor authentication was presented by Das [21] that provide high efficiency. However, this

year the proposed schemes were vulnerable against the man-in-the middle attacks, Song [22] presented the RSA based authentication protocol. Because of the public key storage of sensor nodes and users by this protocol, the proposed method required a lot of storage space.

The user authentication plays a critical role and is necessary for protocols in WSN environments. In 2012 to provide this feature a password-based user authentication scheme in hierarchical WSN proposed by Das *et al.* [23]. Next year, Xue *et al.* [24] suggested a lightweight temporal-credential based mutual authentication. They also claimed that the proposed protocol could withstand various attacks such as stolen smart card attacks, masquerade attacks, and replay attacks.

In the years 2014 and 2015, two teams of researchers present their research on the security of WSN. In the first year, Turkanovic *et al.* [25] provided user authentication and key agreement protocol for heterogeneous ad hoc wireless sensor networks and the second a secure temporal-credential based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks was presented by He *et al.* [26].

In 2016, for a distributed cloud environment architecture, Amin and Biswas [27] presented an authentication protocol using smart cards. In this scheme, the registered users can access private information in safe conditions from all private cloud servers. Also, they claimed that there are two types of security flaws in Turkanovic *et al.*'s protocol [25] and they have the ability to cover up these security weaknesses. Das *et al.* [28] used three-factor user authentication technique to proposed an efficient multi-gateway and key agreement protocol for hierarchical wireless sensor networks.

In 2017, A key exchange protocol improved by Farash *et al.* [29]. they proposed a three-party password-based authenticated key exchange schema that using extended chaotic maps. Mohit *et al.* proposed an authentication protocol for wireless sensor networks [30]. this schema is based on vehicular sensor networks. the same year, Irshad *et al.* [31] proposed authenticated key agreement for multi-server architecture.in this paper, the researchers improved the chaotic map and fixed the security vulnerabilities of Tan's schema [32]. To improve security, a Lightweight Authentication Technique proposed for Heterogeneous Wireless Sensor Networks [57]. Also, they review the security issues of Kalra and Sood schemes.

In 2018, Mishra *et al* [33] proposed an authentication scheme for multimedia communications and designed for IoT environment base on WSN. This schema provides a high efficiency. In the infrastructure that uses the wireless sensor, there are historical security problems.to overcome this kind of security issues Fan Wu *et.al* [34] proposed a lightweight authentication scheme for WMSNs.it addresses the common security requirements and user untraceability. To ensure confidentiality and security in IOT, a biometric-based authentication and key agreement protocol proposed for wireless sensor networks [58].

Recently, researchers have introduced several important authentication protocols and key agreements in the field of wireless sensor network security. Shin, S., & Kwon [35] describe the security weaknesses of Jung *et al.*'s scheme [36] and proposed a lightweight authentication based on the three-factor technique and key agreement protocol for WSN. the proposed scheme addresses several security requirements and uses XOR and hash functions. Naresh *et al.* [37] proposed a lightweight multiple shared key agreement for wireless sensor networks that is based on hyper elliptic curve Diffie–Hellman. the protocol decreases keys exchange overhead and increases the safety of the keys. a lightweight password-authenticated key exchange proposed by González *et al.* [38] for heterogeneous wireless sensor networks. they analyzed three recently proposed 3-PAKE protocols and described the vulnerabilities of the protocols. their novel 3-PAKE protocol provides security features, that are provably secure, flexible and efficient.

III. WEAKNESSES OF MAJID ALOTAIB PROTOCOL

As we all know, the nature of authentication protocols for creating secure communication is providing secure mutual authentication. To provide security Features and Mutual Authentication, MAJID ALOTAIB [39] proposed key agreement protocol based on symmetric cryptosystem and biometric, also, has claimed that his protocol could withstand several security attacks. However, in this section, we demonstrate that his protocol is vulnerable to stolen verify attacks. Also, he clime that his protocol provides perfect forward secrecy, but Contrary to his claim, his method does not meet the security requirements. The details are as follows.

A. STOLEN VERIFY ATTACK

The stolen-verifier attack means that the intruder has stolen the verifier data, long terms data. this attack allows the attacker to access the authentication parameters or important information stored in the server's database, sensor, gateway or IoT device. The provided resistance in MAJID ALOTAIB protocol [39] is not enough and the stolen verify attack can perform by the attacker. The proposed schema uses the symmetric key to encrypt the messages.in the first step of the protocol, the user should generate the symmetric key K and he/she needed to parameters V, T_1, DID_i, Reg_i ($K=h(Reg_i||DID_i||V||T_1)$.this symmetric key generated and shared between GWN and User. Parameter V stored in GWN and as mentioned to the stolen-verifier attack, the attacker can access the parameter V. Other effective parameters (T_1, DID_i, Reg_i) in the symmetric key generation are sent to the unsecured channel and the attacker can access them. So, the symmetric key between the GWN and User can be generated by attacker. in step 4 of protocol, GWN sends the session key to the user by message D_i and this message was encrypted by symmetric key k. Since the attacker has been able to compute the symmetric key K in the first step, it can capture and decrypt the message D_i in the last step. finally, the attacker can access to the session key.

TABLE 1. Symbol Definition of the proposed protocol.

Symbol	Definition
ID_i	User Identity
SID_i	Sensor Identity
S	Gateway Private key
X	Gateway Public key
T_i	Time stamp
PW_i	User Selected Password
SK_i	Session key
H	Hash Function
E_k	Encryption by Summitry key

B. PERFECT FORWARD SECRECY

This feature states that if long-term parameters, including IDs, keys and any other long parameters are disclosure under certain conditions, there is no possibility for the attacker to access or compute the session key. this section presentation that the MAJID ALOTAIB protocol [39] exposing the shared symmetric key GWN and User leads the session key at risk. The details are as follows.

First, By exposing the symmetric key, the attacker can achieve to parameter Regi, DID_i, V, T_1 that they are encrypted by the symmetric key and in step 4 of protocol GWN send D_i to user that is encrypted by symmetric key. this message includes parameters DID_i, SID_n, SK, R_1, T_4. with this condition, the attacker gain to the session key and other long terms such as V, SID_n, R_1.

Second, the attacker capable to generate the symmetric key by having parameter V that mentioned previously, and According to the described conditions, the attacker has obtained parameter V.

In addition to the two significant attacks mentioned above, there are some other weaknesses and these are as follows.

1- the session key generated by the sensor node and transmitted user by GWN. this circumstance raises security issues.

2- There is no registration phase for the sensor node in the article, however, the article [39] states that the sensor node and gateway share the shared symmetric key X_s and sensor ID (SID_n).

3- Biometric has a powerful potential to provide security and authentication mechanism but it has vulnerabilities and is delicate to threats [40], [41].

IV. THE PROPOSED SCHEMA

In this section, we introduced our proposed protocol. The proposed protocol consists of three-phase, two authentication phase and password change, which we will discuss in detail follow table 1 shows the protocol symbols.

A. USER AND GWN REGISTRATION PHASE

In this stage, User selects the identity (ID_i), Password (PW_i) and a random number qi, then compute APW_i.

$$APW_i = h(q_i||PW_i)$$

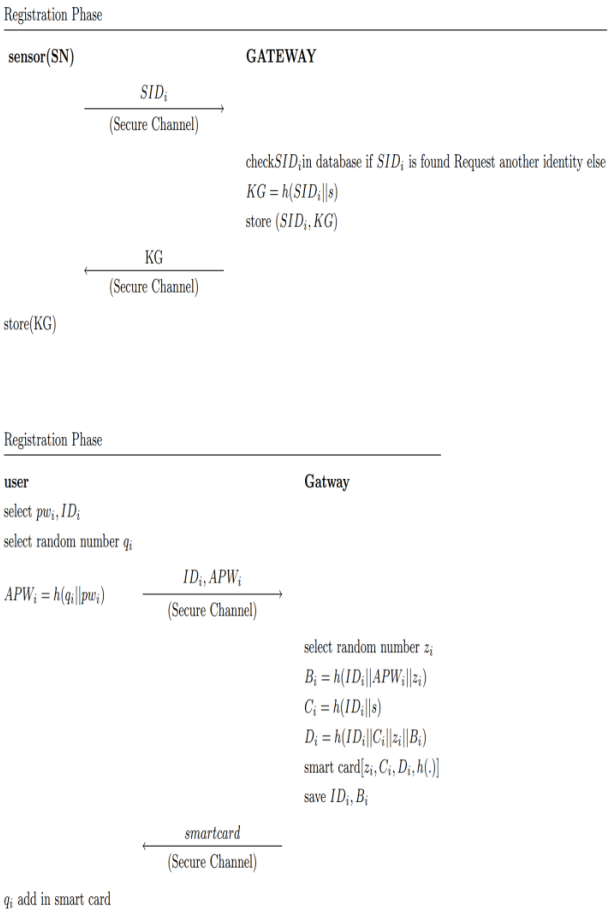


FIGURE 2. Entities Registrations phases.

After computing the APW_i, send it with ID_i to the GWN in secure channel. The gateway first selects a random number Zi as soon as the parameters are received from the user. Second, generate parameters B_i, C_i, D_i.

$$B_i = h(ID_i||APW_i||Z_i), \quad C_i = h(ID_i||s),$$
$$D_i = h(ID_i||C_i||Z_i||B_i)$$

After generating the parameters, store them in the smart card and send it to the user in secure channel. Also, parameters B_i and ID_i stored in GWN. Figure 2 shows the Registrations phases of the User, GWN and Sensor.

Note that, when user received the smart card stored parameter q_i in it.

B. SENSOR AND GWN REGISTRATION PHASE

This phase of registration, sensor and GWN exchange the parameters as follow.

Sensor send his identity (SID_n) to GWN.in the first step Gateway check the sensor identity if it is valid, the GWN generate KG. Finally, GWN send the KG to the sensor and store the parameters SID_n and KG.

$$KG = h(SID_n||s)$$

C. KEY AGREEMENT AND AUTHENTICATION PHASE

After completing the entities' registration steps, the authentication and key exchange phase begins. Figure 3 illustrate the key agreement and Authentication phase.

Step 1. The user inserts the smart card in to the card reader and enters his/her username and password. The following values are calculated after the user enters the parameters.

$$APW_i^* = h(PW_i^*||q_i), \quad B_i^* = h(ID_i^*||APW_i^*||z_i),$$
$$D_i^* = h(ID_i^*||C_i||z_i||B_i^*)$$

These values are generated to verify the parameters that entered by user and uses for mutual Authentication between User node and GWN. First, smart card checked the accuracy of the parameter D_i^*. After generation the parameter D_i^*, it compared with the value D_i that stored in the smart card, and if it is correct, the next steps are performed. The first step after checking the correctness the values a random number a_i selected. then A_1 and A_2 generated by using the a_i.

$$A1 = a_i.p, A_2 = a_i.X$$

NeXT, A time stamp selected as T_1 and the DID_i, A_3,A_4 values generated to create message for GWN.

$$DID_i = ID_i \oplus A_{2(x)},$$
$$A_3 = SID_i \oplus A_{2(x)},$$
$$A_4 = E_{A2}(B_i, SID_i, A_3)$$

Note: A_2 is a point and $A_{2(x)}$ selected base on ECDH as mentioned in Basic Concept section.

Finally, the A_1, A_3, A_4, T_1 sent for GWN in insecure channel.

Step 2. the GWN verifiers $|T2 - T1| < \Delta T$ to checking the message freshness If the confirmation fails, it stops the session. otherwise, computes A2 and decrypts the received message to computing the A3. To verify the received message, the gateway compares the received value of A3 with the A3 that computed and If correct, the work continues. Afterward, the GWN selects a random number gi and compute the following values.

$$KG = h(SID_i, s), D_1 = KG \oplus A_2, D_2 = h(A_2||SID_i||A_3)$$

Finally, GWN forward the $g_i.p$, D_1, D_2, T_2 to the sensor nod through an insecure channel.

Note: Based on ECDH, the generated value A2 by the user is equal to the generated value A2 by the gateway. (user $A_2 = a_i.X =$ GWN $A_2 = s.A_1$)

Step 3. the sensor verifies whether $|T3 - T2| < \Delta T$ is correct of not base on the T3. If the verification does not prop, the session aborted; otherwise, computes $A_2 = KG \oplus D_1$, $A_3 = SID_i \oplus A_{2(X)}$, $D_2^* = h(A_2||SID_i||A_3)$. If $D_2^* \neq D_2$, the sensor rejects the connection. Otherwise, it goes to the next step. Upon proving the authenticity of the GWN, the sensor selects random number y_i, computes $SK_s = h(A_2||f_i.g_i.p)$ and $X_i = h(A_3||KG)$. Lastly, parameters $f_i.p$, X_i, T_3 sends to the GWN by the sensor.

Note: as mentioned in basic concept section an attacker cannot capable to calculate $f_i.g_i.p$ with values of $g_i.p$ and $f_i.p$.

Step 4. The Gateway checks the message freshness by computing $|T4 - T3| < \Delta T$ and if it is incorrect the session dropped, otherwise the next step taken. Authenticating the sensor by the gateway is considered as the next step.it is performed by computing $X_i^* = h(A_3||KG)$ and compare with the received X_i in insecure channel. If $X_i^* \neq X_i$ the GWN aborts the connection, otherwise, Otherwise, the sensor is an authorized entity and the gateway generate the following values.

$$D_4 = E_{A2}(g_i), y_i = h(T_4||A_3), D_5 = h(y_i||A_3)$$

Ultimately, the GWN sends parameters $f_i.p$, D_5, D_4, T_4 to the user in insecure channel.

Step 5. After receiving the message, the User select T_5 and checks the message freshness condition $|T_5 - T_4| < \Delta T$. If the freshness verification does not hold, aborts the session; otherwise, the D_4 is decrypted to reach g_i and to authenticate the GWN, user computing $y_i = h(T_4||A_3)$ and $D_5^* = h(y_i||A_3)$. After calculating the values, D_5^* compare with received D_5. If $D_5^* \neq D_5$ the connection dropped and if it is true the session key computed by user as follow.

$$SK_u = h(A_2||f_i.g_i.p)$$

D. PASSWORD CHANGE PHASE

The security protocols that use password-based authentication, an authorized user needed to be able to update the PWi, so in this circumstance, the protocol requires a password change mechanism. The password change steps are as follows.

Step 1. The user inserts his/her smart card and enter his/her ID_i and PW_i. Then the following operation executes to generate D_i and verified the entered PWI.

$$APWi_i^* = h(PW_i^*||q_i), \quad B_i^* = h(ID_i^*||APWi_i^*||z_i),$$
$$D_i^* = h(ID_i^*||C_i||z_i||B_i^*, D_i = ?D_i^*$$

Step 2. User request the password change and enter the new PW_i. After that, the APW_{ii}^{**}, B_i^{**} and D_i^{**} values are made. Finally, the Di** replaced instead of Di* and store in smart card.

V. OFFICIAL SECURITY PROOF WITH SCYTHER

Scyther [42] is a powerful and effective tool for analyzing, identifying potential attacks and vulnerabilities of security protocols. These official tools automatically analyze the protocol and scrutinize its behavior against most possible attacks. Researchers have used this tool to prove the security of their proposed methods [59], [60]. Figure 4 shows the output of the scyther proposed protocol review. Niagree's feature ensures that the parties to the communication are assured that the messages are transmitted securely and in the correct order between them. Also, this feature ensures that the transmitted message between the parties unable to decrypt and resubmit. The Alive feature ensures that the protocol steps are approved

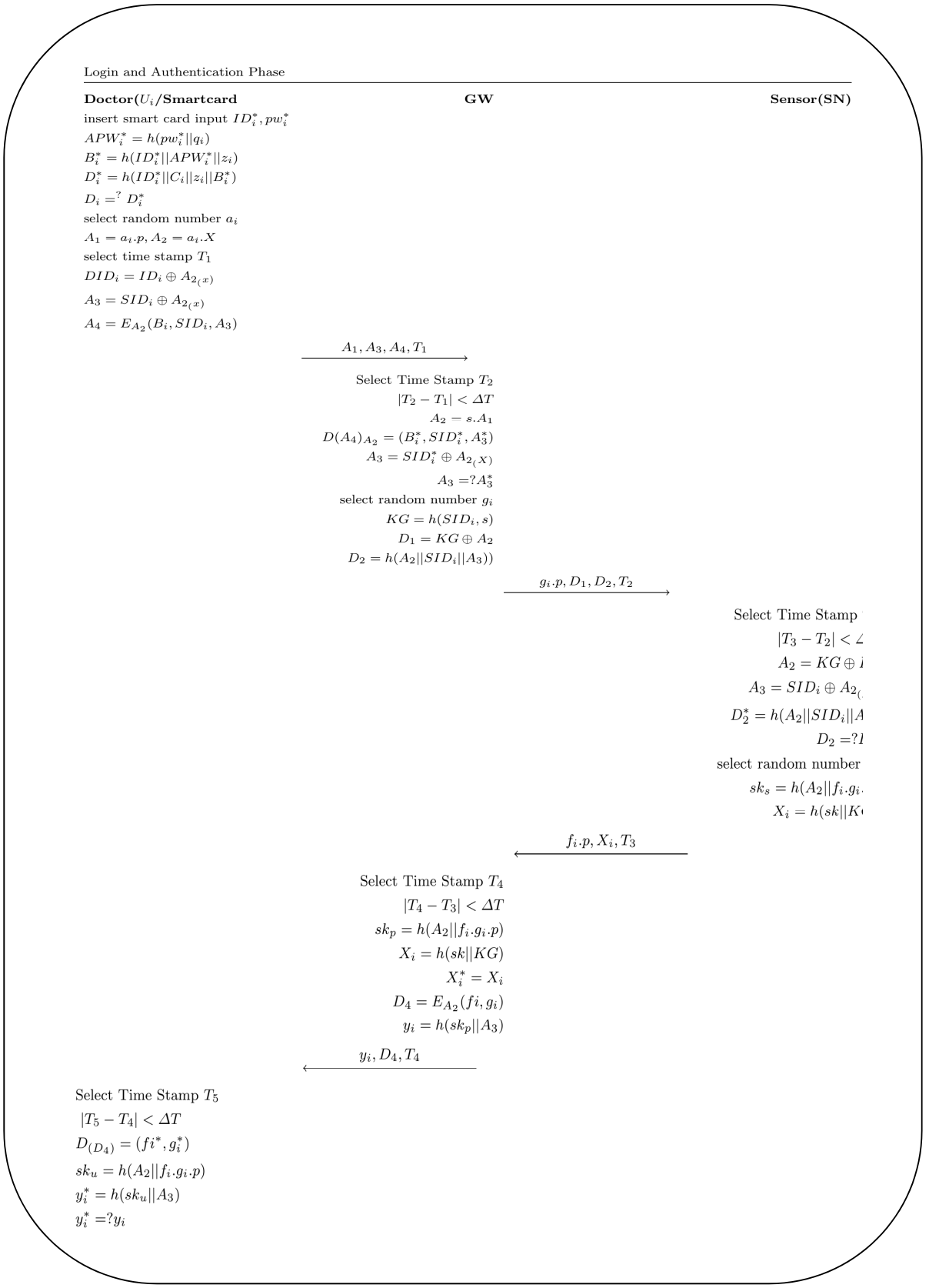
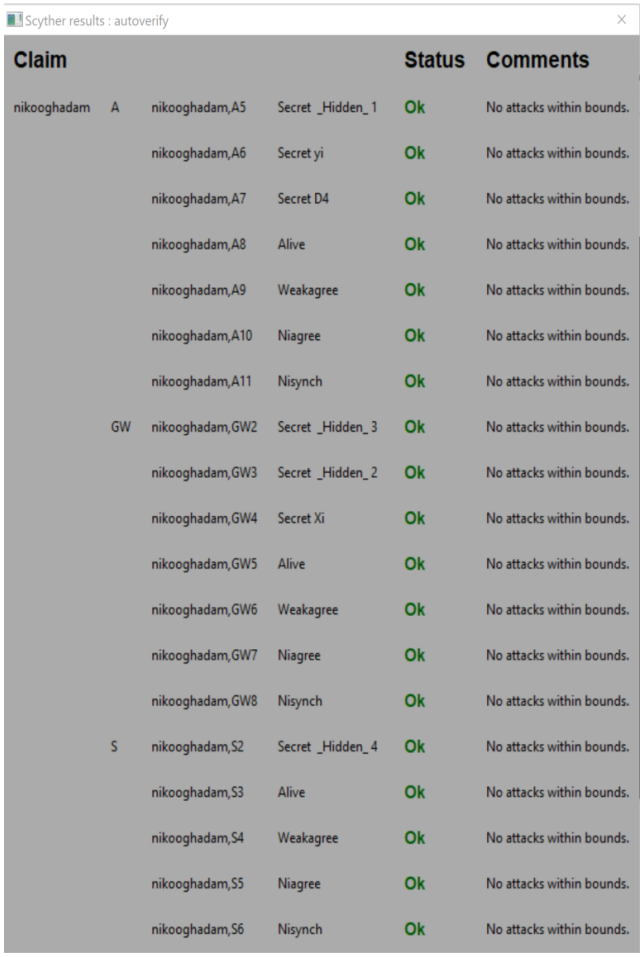


FIGURE 3. Key agreement and Authentication phase.


Scyther results : autoverify

Claim				Status	Comments
nikooghadam	A	nikooghadam,A5	Secret _Hidden_1	Ok	No attacks within bounds.
		nikooghadam,A6	Secret yi	Ok	No attacks within bounds.
		nikooghadam,A7	Secret D4	Ok	No attacks within bounds.
		nikooghadam,A8	Alive	Ok	No attacks within bounds.
		nikooghadam,A9	Weakagree	Ok	No attacks within bounds.
		nikooghadam,A10	Niagree	Ok	No attacks within bounds.
		nikooghadam,A11	Nisynch	Ok	No attacks within bounds.
	GW	nikooghadam,GW2	Secret _Hidden_3	Ok	No attacks within bounds.
		nikooghadam,GW3	Secret _Hidden_2	Ok	No attacks within bounds.
		nikooghadam,GW4	Secret Xi	Ok	No attacks within bounds.
		nikooghadam,GW5	Alive	Ok	No attacks within bounds.
		nikooghadam,GW6	Weakagree	Ok	No attacks within bounds.
		nikooghadam,GW7	Niagree	Ok	No attacks within bounds.
		nikooghadam,GW8	Nisynch	Ok	No attacks within bounds.
	S	nikooghadam,S2	Secret _Hidden_4	Ok	No attacks within bounds.
		nikooghadam,S3	Alive	Ok	No attacks within bounds.
		nikooghadam,S4	Weakagree	Ok	No attacks within bounds.
		nikooghadam,S5	Niagree	Ok	No attacks within bounds.
		nikooghadam,S6	Nisynch	Ok	No attacks within bounds.

FIGURE 4. The results of analyzing the proposed protocol using the SCYTHER tool.

by the parties to the communication. The Weakagree feature ensures that there is no possibility for attacker to performing an impersonation attack.

VI. INFORMAL SECURITY ANALYSIS OF THE PROPOSED PROTOCOL

A. SECURE AGAINST THE REPLY ATTACK

Due to the use of timestamps in the proposed protocol as well as the random numbers, the attacker can not be able to send duplicate messages. Suppose that the adversary eavesdrops a message and try to send it again in a different session, But there are two obstacles for the attacker, time stamp that checks every step and random number for every entity. timestamp helps to check the freshness of messages and random numbers made unique values for every session.

B. SECURE AGAINST THE DOS ATTACK

An attacker with this kind of attack trying to send messages frequently and sequentially and his/her aim is that deactivate the server. In the proposed protocol, if the attacker repeats messages that are transmitted over the public and unsecured channel and sends a large number of the messages to the server sequentially, Because of the random numbers as well as the time stamp in the protocol, the message recipient recognizes duplicate messages and drop the connection.

C. SECURE AGAINST KNOWN-SESSION-SPECIFIC TEMPORARY INFORMATION ATTACK

Since at the registration stage, the user does not explicitly And sends it to the server in the form of $APW_i = h(q_i \,||\, PW_i)$, so even if a personal attacker is inside the server, there is no possibility of an internal attack.

D. SECURE AGAINST THE STOLEN VERIFY ATTACK

The attack assumes that if the attacker is able to access the parameters stored in memory, he/she can not be possible to access the session key. In the proposed method, if the attacker can access the parameters stored in the gateway, he/she cannot access the session key and the symmetric key. Suppose that under certain circumstances the attacker was able to access the parameters stored in the gateway (B_i,C_i,D_i). As can be seen in the proposed schema, the session key and the symmetric key are generated based on the ECDH technique. It also requires parameters g_i, f_i and A_2 to generate keys, which are random numbers and variable parameters, most importantly they are not stored in any entities.

E. PROVIDE SECURITY CONDITION FOR SESSION KEY

This security requirement states that only the session key generating party must be able to access it. the attacker can not be able to access the session key through the public key and the parameters exchanged on the public channel. there is no possibility for the attacker to gain the session key. For example, session key equation is $SK = h(A_2||f_i.g_i.p)$ and $g_i.p$, f_i,p are sent in an unsecure channel. Base on the ECDH that mention in basic concept section, the attacker can not be able to computing or achieving the session key.

F. PERFECT FORWARD SECRECY

The proposed protocol uses elliptic curve cryptography and ECDH theorem. parameter A_2 is used to generating the symmetric key and for generating the A_2, a random number is used.so the symmetric key is unique for every session a completely different. also, this unique feature is considered for the session key. The proposed protocol uses the parameter g_i, f_i, and A_2 to generate session key. Parameters g_i and f_i are the random numbers and as mentioned A2 is completely different for each session.so the random numbers and A_2 made the session key unique for each session. But the significant point is that, if the attacker can access the long term of the proposed protocol such as the GWN secret key there is no way to achieving the session key. this is because of the ECDH features and random number f_i, g_i that mentioned before.

G. SECURE AGAINST EXPOSING THE RANDOM PARAMETERS

The assumption in this type of attack is that if the random parameters disclosure and reach the attacker. He/she should

not be able to achieve the established session key between the parties. Suppose that all the random parameters in the protocol are exposed. Since parameter A_2 is used to generate the session key and it is made from the secret key of the user, even with exposing the random parameters of the protocol, it is impossible to access the session key.

H. SECURE AGAINST OFFLINE PASSWORD GUESSING ATTACKS:

Assume that the adversary Obtained under certain conditions access to the user's smart card and retrieves $< D_i, C_i, B_i, z_i >$ from the memory of the smart card. there is no possibility for an attacker to guessing the APW_i, because a random number chose to generate the APW_i and this parameter is used for generating the B_i, D_i. Therefore, the proposed protocol can withstand the password guessing attacks.

I. SECURE AGAINST MAN-IN-THE-MIDDLE ATTACKS:

In this attack, the attacker secretly intercepts, relays a message or alters the communication between two entities. In the proposed protocol, an efficient mutual authentication mechanism, ECDH based authentication and symmetric cryptography based on ECDH is considered. In the first handshake of protocol if an attacker wants to perform Man-in-the-middle attacks needed to accesses the A1, A2 and the symmetric key. To generate the A1 and A2 the attacker requires the random number ai and user private key (X), these parameters are completely secret for user and attacker can not access them. Also, to achieving the symmetric key needed to generate A2 because the symmetric key generated based on ECDH. Finally, in the proposed protocol There are no conditions for the Man-in-the-middle attack.

VII. PERFORMANCE ANALYZE

This section evaluated the proposed protocol and other related protocols, also they compared base on security feature and computation. The evaluation results are reported to present the security feature of the proposed protocol.

A. SECURITY AND FUNCTIONALITY COMPARISON

this section is presented to compare the proposed protocol with other protocols. For this purpose security attacks and functionality requirements are shown in Table 2. As seen in table 2,the proptocol in [39], [45], [49], [34], [55] are vulnerable to Stolen verify attack and protocol in [51], [56] are suffer from Impersonation attack.

Furthermore, the protocols in [56], [39] do not provide perfect forward secrecy features. while the proposed scheme is more efficient and provides an important security feature in WSN environment.

B. COMPUTATIONAL COST COMPARISON

In this part of the performance analysis section, we compare the proposed protocol schema computation cost with other protocols. The registration and password change phases are not performed frequently, so the cost of login and authentication phases focused and compared. Also, the execution time of XOR operation is negligible and we do not consider it for computation cost. to comfort analysis, the symbols are used. The computation time for each cryptographic operation and the notations are mentioned in Table 3 [54].

We compared the proposed schema with other rated protocols. As can be noticed, the computation time of our protocol is less among all existing schemes.

The incurs computation cost of our scheme for login and authentication phases is $13T_h+5T_{ECC}+3T_{sym} = 0.10646$ seconds. Table 4 and Figure 5 show the efficiency of our proposed scheme in the field of computation cost against the related protocols. The performance comparison illustrates that the proposed protocol takes lower computation and provides complete security. Also, to describe the communication cost, table 5 shows the handshakes and the number of bits per message. The communication cost of sending identity is considered to be 160 bits, the timestamp is 32 bits, encryption/decryption operations are 128 bits, elliptic curve point multiplication is 320 bits, the realm is 32 bits, and a random number and output hash function are 32 and 160 bits, respectively.

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

Security attributes	[34]	[52]	[55]	[45]	[49]	[56]	[51]	[39]	Our
Resists Reply Attack	Y	Y	Y	Y	Y	Y	Y	Y	Y
User anonymity	N	Y	Y	N	N	Y	Y	Y	Y
Mutual Authentication	Y	N	Y	Y	Y	Y	Y	Y	Y
Resists Stolen verify attack	N	Y	N	N	N	Y	Y	N	Y
Resists Stolen smart card	N	Y	N	N	N	Y	Y	N	Y
Resists Impersonation attack	Y	Y	Y	Y	N	N	N	Y	Y
Resists Man in the Middle	Y	Y	Y	Y	N	Y	Y	Y	Y
Session key agreement	Y	Y	Y	Y	Y	Y	Y	Y	Y
Resists Danial of Service	N	Y	Y	Y	Y	Y	Y	Y	Y
Perfect forward secrecy	Y	Y	Y	Y	Y	N	Y	N	Y
Resist known session-specific temporary information attack	N	N	-	N	-	N	N	N	Y
Resists privileged insider attack	Y	Y	Y	Y	Y	Y	Y	Y	Y
Resist identity reveal attack	N	N	Y	N	-	Y	Y	Y	Y
Resists forgery attack	-	-	Y	N	N	N	N	Y	Y

TABLE 3. Time required for various operations.

Notation	Description	Computation time (in seconds)
T_h	Hash function	0.00032
T_{ECC}	ECC point multiplication	0.0171
T_F	Fuzzy extractor function	0.0056
T_{sym}	Symmetric encryption/decryption	0.0171

TABLE 4. Computation comparison during the login and authentication phases.

Schema	User	Gateway	Sensor	Total	Time (in seconds)
[44]	$5T_h+3T_{ECC}$	$8T_h+T_{ECC}$	$4T_h+2T_{ECC}$	$17T_h+6T_{ECC}$	0.10804
[45]	$8T_h+3T_{ECC}$	$5T_h+T_{ECC}$	$6T_h+2T_{ECC}$	$19T_h+6T_{ECC}$	0.10868
[46]	$4T_h+T_{sym}+3T_{ECC}$	$4T_h+2T_{sym}+T_{ECC}$	$3T_h+2T_{ECC}$	$12T_h+3T_{sym}+6T_{ECC}$	0.12324
[47]	$1T_h+2T_{ECC}$	$4T_h+4T_{ECC}$	$3T_h+2T_{ECC}$	$8T_h+8T_{ECC}$	0.13936
[48]	$15T_h+3T_{ECC}+1T_F$	$11T_h+3T_{ECC}$	$7T_h$	$T_F+6T_{EC C}+31T_h$	0.12962
[49]	$10T_h+T_F+T_{sym}+2T_E$	$10T_h+2T_{sym}$	$6T_h+T_{sym}+2T_E$	$26T_h+T_F+4T_{ECC}+4T_{sym}$	0.11622
[50]	$5T_{ECC}+5T_h$	$5T_{ECC}+4T_h$	$4T_{ECC}+3T_h$	$14T_{ECC}+12T_h$	0.24344
[51]	$6T_h+3T_{ECC}+1T_F$	$6T_h+1T_{ECC}+1T_{sym}$	$4T_h+2T_{ECC}+1T_{sym}$	$16T_h+6T_{ECC}+2T_{sym}$	0.11892
[52]	$8T_h+3T_{ECC}$	$7T_h+T_{ECC}$	$4T_h+2T_{ECC}$	$19T_h+6T_{ECC}$	0.10868
[53]	$5T_h+T_{ECC}+2T_{sym}$	$5T_h+4T_{ECC}2T_{sym}$	$1T_h+1T_{ECC}2T_{sym}$	$11T_h+6T_{ECC}+6T_{sym}$	0.13972
Our	$6T_h+3T_{ECC}+1T_{sym}$	$1T_{ECC}+5T_h+2T_{sym}$	$1T_{ECC}+2T_h$	$13T_h+5T_{ECC}+3T_{sym}$	0.10646

TABLE 5. Communication cost.

	Handshake	Bit per message
[39]	4	2144
Our	4	1504

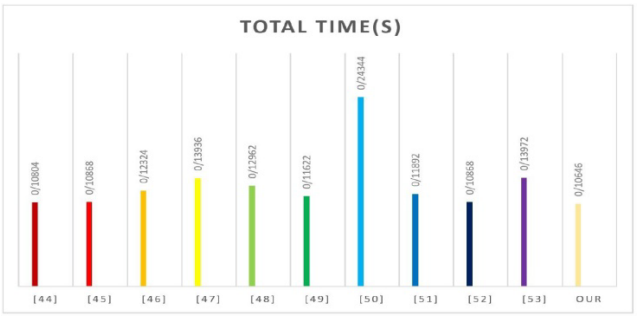


FIGURE 5. Computation comparison during the login and authentication phases.

VIII. CONCLUSION

In this paper, we have analyzed the security drawbacks of MAJED ALOTAIBI symmetric cryptosystem and Biometric-Based Anonymous User Authentication and key agreement protocol. We have identified the vulnerabilities of MAJED ALOTAIBI scheme to Stolen verify attack, impersonation attack, session key security issues, no registration phase for sensor and biometric vulnerability. Furthermore, to addresses the vulnerabilities and create secure communication with authorized entities, we have proposed an ECDH based authentication and key agreement protocol for WSN infrastructure. the proposed protocol supports the dynamic node addition in WSN environments and uses strong ECDH technique to generate unique symmetric key and session key for each session. Using the informal analysis to prove that the proposed protocol performs mutual authentication and other security features. In addition, we have a formal security analysis and use the Scyther tool to demonstrate that the proposed schema is secure against the severe attacks. the Scyther analysis consists of three-part Niagree's feature, Alive feature and Weakagree feature. totally, our proposed protocol performance is more efficient than other related presented protocols and supports extra security attributes.

REFERENCES

[1] Z. Zhang, A. Mehmood, L. Shu, Z. Huo, Y. Zhang, and M. Mukherjee, "A survey on fault diagnosis in wireless sensor networks," *IEEE Access*, vol. 6, pp. 11349–11364, 2018.
[2] A. H. Mohajerzadeh, H. Jahedinia, Z. Izadi-Ghodousi, D. Abbasinezhad-Mood, and M. Salehi, "Efficient target tracking in directional sensor networks with selective target area's coverage," *Telecommun. Syst.*, vol. 68, no. 1, pp. 47–65, May 2018.
[3] S. A. Chaudhry, H. Naqvi, M. S. Farash, T. Shon, and M. Sher, "An improved and robust biometrics-based three factor authentication scheme for multiserver environments," *J. Supercomput.*, vol. 74, no. 8, pp. 3504–3520, Aug. 2018.
[4] M. Nikooghadam, R. Jahantigh, and H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13401–13423, Jun. 2017.
[5] A. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 12, no. 1, pp. 43–59, Jan. 2019.
[6] D. Zhang, Y. Qian, J. Wan, and S. Zhao, "An efficient RFID search protocol based on clouds," *Mobile Netw. Appl.*, vol. 20, no. 3, pp. 356–362, Jun. 2015.
[7] B. Gupta, D. P. Agrawal, and S. Yamaguchi, *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*. Hershey, PA, USA: IGI Global, 2016.
[8] J. Choi, J. Bang, L. Kim, M. Ahn, and T. Kwon, "Location-based key management strong against insider threats in wireless sensor networks," *IEEE Syst. J.*, vol. 11, no. 2, pp. 494–502, Jun. 2017.
[9] M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," *Comput. Commun.*, vol. 134, pp. 52–69, Jan. 2019.
[10] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, pp. 112–126, Dec. 2018.
[11] S. Agrawal and M. L. Das, "Mutual healing enabled group-key distribution protocol in wireless sensor networks," *Comput. Commun.*, vol. 112, pp. 131–140, Nov. 2017.
[12] F. Zhan, N. Yao, Z. Gao, and G. Tan, "A novel key generation method for wireless sensor networks based on system of equations," *J. Netw. Comput. Appl.*, vol. 82, pp. 114–127, Mar. 2017.
[13] S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs," *Future Gener. Comput. Syst.*, vol. 92, pp. 789–799, Mar. 2019.
[14] S.-H. Seo, J. Won, S. Sultana, and E. Bertino, "Effective key management in dynamic wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 371–383, Feb. 2015.
[15] P. Ahlawat and M. Dave, "An attack model based highly secure key management scheme for wireless sensor networks," *Procedia Comput. Sci.*, vol. 125, pp. 201–207, Jan. 2018.
[16] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[17] F. Al-Turjman, Y. K. Ever, E. Ever, H. X. Nguyen, and D. B. David, "Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks," *IEEE Access*, vol. 5, pp. 24617–24631, 2017.
[18] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer, 2006.
[19] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.
[20] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput. (SUTC)*, vol. 1, Jun. 2006, p. 8.
[21] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.
[22] R. Song, "Advanced smart card based password authentication protocol," *Comput. Standards Interfaces*, vol. 32, nos. 5–6, pp. 321–325, Oct. 2010.
[23] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646–1656, Sep. 2012.
[24] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, Jan. 2013.
[25] M. Turkanović, B. Brumen, and 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.*, vol. 20, pp. 96–112, Sep. 2014.
[26] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, Nov. 2015.
[27] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.
[28] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, "An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2070–2092, 2016.
[29] M. S. Farash, M. A. Attari, and 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.*, vol. 30, no. 1, p. e2912, Jan. 2017.
[30] P. Mohit, R. Amin, and G. P. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Veh. Commun.*, vol. 9, pp. 64–71, Jul. 2017.
[31] A. Irshad, "An improved and secure chaotic-map based multi-server authentication protocol based on lu et al. and Tsai and Lo's scheme," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 3185–3208, 2017.
[32] Z. Tan, "A privacy-preserving multi-server authenticated key-agreement scheme based on Chebyshev chaotic maps," *Secur. Commun. Netw.*, vol. 9, no. 11, pp. 1384–1397, Jul. 2016.
[33] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18295–18325, Jul. 2018.
[34] F. Wu, X. Li, A. K. Sangaiah, L. Xu, S. Kumari, L. Wu, and J. Shen, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 727–737, May 2018.
[35] S. Shin and T. Kwon, "A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes," *Sensors*, vol. 19, no. 9, p. 2012, 2019.
[36] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017.
[37] V. S. Naresh, S. Reddi, and N. V. Murthy, "Provable secure lightweight multiple shared key agreement based on hyper elliptic curve Diffie–Hellman for wireless sensor networks," *Inf. Secur. J., Global Perspective*, vol. 29, no. 1, pp. 1–13, 2020.
[38] I. Santos-González, A. Rivero-García, M. Burmester, J. Munilla, and P. Caballero-Gil, "Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks," *Inf. Syst.*, vol. 88, Feb. 2020, Art. no. 101423.
[39] M. Alotaibi, "An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN," *IEEE Access*, vol. 6, pp. 70072–70087, 2018.
[40] A. O. Alaswad, A. H. Montaser, and F. E. Mohamad, "Vulnerabilities of biometric authentication threats and countermeasures," *Int. J. Inf. Comput. Technol.*, vol. 4, no. 10, pp. 58–947, 2014.
[41] P. S. Prasad, "Vulnerabilities of biometric system," *Int. J. Sci. Eng. Res.*, 2013.
[42] C. J. F. Cremers, "Scyther: Semantics and verification of security protocols," Eindhoven Univ. Technol. Eindhoven, The Netherlands, Tech. Rep., 2006.
[43] M. Nikooghadam and H. Amintoosi, "Secure communication in CloudIoT through design of a lightweight authentication and session key agreement scheme," *Int. J. Commun. Syst.*, p. e4332, Feb. 2020.
[44] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *J. Ambient Intell. Hum. Comput.*, vol. 8, no. 1, pp. 101–116, Feb. 2017.
[45] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.
[46] J. Nam, M. Kim, J. Paik, Y. Lee, and D. Won, "A provably-secure ECC-based authentication scheme for wireless sensor networks," *Sensors*, vol. 14, no. 11, pp. 21023–21044, Nov. 2014.
[47] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.
[48] P. Soni, A. K. Pal, and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote healthcare system," *Comput. Methods Programs Biomed.*, vol. 182, Dec. 2019, Art. no. 105054.
[49] Y. Choi, Y. Lee, and D. Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 1, Jan. 2016, Art. no. 8572410.
[50] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.
[51] J. Moon, D. Lee, Y. Lee, and D. Won, "Improving biometric-based authentication schemes with smart card Revocation/Reissue for wireless sensor networks," *Sensors*, vol. 17, no. 5, p. 940, 2017.
[52] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.
[53] M. Nikravan and A. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the Internet of Things," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 463–494, Mar. 2020.
[54] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[55] Y. Park and Y. Park, "Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 12, p. 2123, 2016.
[56] R. Amin, S. K. H. Islam, N. Kumar, and K.-K.-R. Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 104, pp. 133–144, Feb. 2018.
[57] C. S. Vorugunti, B. Mishra, R. Amin, R. P. Badoni, M. Sarvabhatla, and D. Mishra, "Improving security of lightweight authentication technique for heterogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 3141–3166, Aug. 2017.
[58] J. Srinivas, D. Mishra, S. Mukhopadhyay, and S. Kumari, "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks," *J. Ambient Intell. Hum. Comput.*, vol. 9, no. 4, pp. 875–895, Aug. 2018.
[59] R. Amin, P. Lohani, M. Ekka, S. Chourasia, and S. Vollala, "An enhanced anonymity resilience security protocol for vehicular ad-hoc network with Scyther simulation," *Comput. Electr. Eng.*, vol. 82, Mar. 2020, Art. no. 106554.
[60] R. Amin, S. Kunal, A. Saha, D. Das, and A. Alamri, "CFSec: Password based secure communication protocol in cloud-fog environment," *J. Parallel Distrib. Comput.*, vol. 140, pp. 52–62, Jun. 2020.

MOSTAFA FARHADI MOGHADAM received the B.S. degree in computer from the University of Applied Science and Technology, Mashhad, Iran. He is currently pursuing the M.S. degree with Imam Raza University (IRU), Mashhad. He researches on smart grid and cryptography. He is also a Teacher Assistant with the Vahdat Institute of Higher Education.

MAHDI NIKOOGHADAM received the B.Sc. degree in information technology (IT) from the Sadjad University of Technology, Mashhad, Iran, in 2018. He is currently pursuing the master's degree in computer engineering with the Fredowsi University of Mashhad. His research interests include information security, cryptography, and security protocols.

MAYTHAM AZHAR BAQER AL JABBAN received the B.S. degree from Iraq Universities and the M.S. degree from the Ferdowsi University of Mashhad, Iran, in 2014 and 2018, respectively, where he is currently pursuing the Ph.D. degree. He has computer network engineering with security and the Internet of Things (IoT). He has an article with subject (A Group Authentication Protocol On Multilayer Structure For Privacy-Preserving IoT Environment).

MOHAMMAD ALISHAHI, photography and biography not available at the time of publication.

LEILI MORTAZAVI, photography and biography not available at the time of publication.

AMIRHOSSEIN MOHAJERZADEH received the B.S., M.S., and Ph.D. degrees from the Ferdowsi University of Mashhad, Mashhad, Iran, in 2005, 2007, and 2013, respectively. He has been a Computer Network Engineer with several networking projects at the Iran Telecommunication Research Center (ITRC), since 2008. He is the author of one book in Farsi language in networking field. He is currently an Assistant Professor with the Computer Engineering Department, Ferdowsi University of Mashhad. He has published more than 30 international conference and journal articles. His research interests are in cellular networks (5G), wireless sensor networks (WSNs), software-defined networking (SDN), smart grid, target tracking, modeling and analyzing computer networks, Quality of Services (QoS) and fuzzy logic control.