The ISC Int'l Journal of Information Security

ISeCure

July 2019, Volume 11, Number 2 (pp. 113–128)

http://www.isecure-journal.org

A Lightweight Privacy-preserving Authenticated Key Exchange Scheme for Smart Grid Communications

Majid Bayat [1,*], Zahra Zare Jousheghani [2], Ashok Kumar Das [3], Pitam Singh [4], Saru Kumari [5], and Mohammad Reza Aref [2]

[1] *Department of Computer Engineering, Shahed University, Tehran, Iran*
[2] *Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran*
[3] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India*
[4] *Department of Mathematics, Motilal Nehru National Institute of Technology (MNNIT), Allahabad, Uttar Pradesh, India*
[5] *Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India*

ARTICLE INFO.

Article history:
Received: 15 December 2018
Revised: 9 July 2019
Accepted: 13 July 2019
Published Online: 31 July 2019

Keywords:
Smart Grid, Authentication, Privacy Preserving, AVISPA, BAN Logic.

Abstract

Smart grid concept is introduced to modify the power grid by utilizing new information and communication technology. Smart grid needs live power consumption monitoring to provide required services and for this issue, bi-directional communication is essential. Security and privacy are the most important requirements that should be provided in the communication. Due to the complex design of smart grid systems, and utilizing different new technologies, there are many opportunities for adversaries to attack the smart grid system that can result fatal problems for the customers. Recently, Mahmood *et al.* [1] proposed a lightweight message authentication scheme for smart grid communications and claimed that it satisfies the security requirements. We found that Mahmood *et al.*'s scheme has some security vulnerabilities and it has not adequate security features to be utilized in smart grid. To address these drawbacks, we propose an efficient and secure lightweight privacy-preserving authentication scheme for a smart grid. Security of our scheme are evaluated, and the formal security analysis and verification are introduced via the broadly-accepted BAN logic and AVISPA tool. Finally, the security and efficiency comparisons are provided, which indicate the security and efficiency of the proposed scheme as compared to other existing related schemes.

1 Introduction

In the past decades, the development of power networks has not been synchronized with social and industrial development. For instance, the statistics show that the energy production was doubled but the energy consumption was tripled between 1950 and 2008 [2]. This increasing demand on the power system has led to an important challenge in the proper management domain of various energy resources, such as fossil fuels and renewable energy resources [3]. On the other hand, due to the lack of an effective method of detecting and repairing defects, the traditional power systems are suffering from power outage and

* Corresponding author.
Email addresses: mbayat@shahed.ac.ir, zarejousheghani_zahra@alum.sharif.edu, ashok.das@iiit.ac.in, pitams@mnnit.ac.in, saryusiirohi@gmail.com, aref@sharif.ir

ISSN: 2008-2045

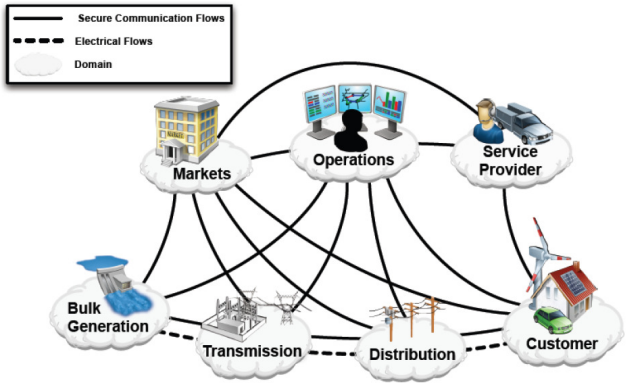

Figure 1. A smart grid architecture [8]

blackouts occasionally. For instance, on August 14, 2003, a cascade of failures happened throughout the southeastern Canada and northeastern U.S. which makes the biggest blackout in the American history. This big blackout contributed in losing power for up to two days for 50 million people, 11 deaths and $6 billion loss in economic revenue [4]. After such incidents, information and communication based power system is considered as a solution for these problems, which is called smart grid [5]. Compared to the traditional power systems, smart grids have emerged with interesting features, such as data representation, self-healing and remote monitoring [6]. There is only one-way electricity flow in the traditional power systems, while we have two-way electricity and information flow in the smart grids. Hence, smart grids are expected to emerge as the next generation of power grids and they absorb both of the power and communication engineers [7].

Based on an architecture model which was proposed by the National Institute of Standards and Technology (NIST) of the United States [8], smart grids consist of seven logical domains, including bulk generation, transmission, distribution, customer, market, service provider and operation domains. According to Figure 1, the first four domains contain the two-way energy and information transmission, and the last three domains are introduced for collecting information and managing energy in smart grids [8]. Due to the importance of high-speed transmission of data between the smart grid domains, the communication technology used throughout this network is fiber-optic, except in the customer domain. Usually, wireless network is used for the communication in the customer domain to reduce the cost and complexity for the consumers [3].

As it can be seen in Figure 1, smart grid is basically an information communication network which is gathered with power system and manages all parts of the cyber-physical network based on the received real-time data about the power demand, consumption, transmission and distribution [9]. Therefore, the accurate performance of this smart network has a great dependence on the accuracy and timeliness of transmitted data through the network. This dependency on the data makes this system extremely vulnerable to cyber attacks [3, 10–12]. Moreover, according to the report provided by the power electronics research institute [13], the cyber security issues of the smart grid are the most important existing challenges for implementation and development of this network on the wide scale. Hence, the NIST has provided a detailed guideline for the smart grid cyber security requirements [14]. In the following, we explain some of its most important security-requirements briefly.

- Confidentiality: This property gets much attention to prevent unauthorized disclosure of information and privacy preserving of individuals in recent decades.
- Accessibility: This is one the most important feature in the smart grids which ensures the reliable and well-timed access to information.
- Integrity: It is responsible for preventing unauthorized alternation of information, and also it causes the validity and non-repudiation of the information in the network.
- Authentication: It is a key process for verifying the identity of devices and individuals, and also is known as a prerequisite for granting access to resources in the network. Therefore, the accessibility of unauthorized nodes to the information is restricted.

The existence of a secure appropriate method for authentication is one of the most significant challenges to achieve an acceptable security level in smart grids [15]. Several authentication methods for smart grids have been introduced till now which each of them has its own advantages and disadvantages. One of these methods which is more suitable for this network was proposed by Mahmood *et al.* [1]. In Mahmood *et al.*'s scheme, two parts of the network, namely home area network and building area network, are authenticated to each other through hybrid cryptography and also establish a shared session key between themselves. After that, those two parts can communicate and transmit messages by using the mentioned shared session key. This scheme has low communication and computational overheads in comparison with other existing schemes which make it more appropriate for the environment with limited resources such as smart grid. Besides that, it is resistant against man-in-the-middle and replay attacks. Despite all of the advantages of this mentioned method, we have investigated that it suffers from some vulnerability issues, such as key compromise impersonation (KCI) attack, forward

secrecy and privacy-preservation.

1.1 Related Work

As the authentication is one of the most important security properties in the smart grid, a lot of authentication schemes in this domain are proposed till now which we analyze some of them in this section. These studied schemes are utilized different public key cryptosystem methods, such as Merkle hash tree [16], one time signature [17], elliptic curve cryptography [18], Identity-Based cryptography [19], Diffie-Hellman exchange protocol [20] and so on which each of these methods has their own pros and cons. We briefly explain our studied schemes in the following.

The Merkle tree based authentication schemes which are proposed in [7] and [21] uses hash functions instead of PKI such as discrete logarithm or integer factorization to provide an authentication scheme with an appropriate security level despite the advent of quantum computers. Besides that, these schemes are resistant against some of the important attacks such as replay attack, message injection attack, message analysis attack, message modification attack and so on. Since the computations of the mentioned schemes are based on the hash functions, they have low computation and communication overheads and high speed which means low computation time, but they have high latency and require more memory space, because of the numerous number of nodes in each tree.

In many cases, control center requires to send a message to a group of consumers. For example in the event of a crisis, it requires to interrupt the power of a region by sending a message to all the consumers in that region. In these cases, a multicast communication is needed instead of unicast communication. As it is stated in [22], one method of establishing multicast communication is the use of one time signature. Besides that, since one time signature method is able to allocate computations between sender and receiver nodes in accordance with their computational resources, the other important feature of this method is its flexibility. Computational overhead, computational time and required memory space are allocated proportional to sender and receiver computational power. But, because of using signature in this method, it has high latency and communication overhead.

As it is mentioned in [23], communications in smart grid are very sensitive to the latency of data transmission. Therefore, the use of authentication protocol based elliptic curve cryptography is one of the most important methods to minimize this latency. The mentioned two-way authentication scheme in [23] has high computational overhead and computational time but its communication overhead, latency and required memory space are so low.

In [24], the identity based cryptography is used to propose an authentication scheme, therefore this scheme does not require any certificate authority. Indeed, a secure server executes the responsibilities of certificate authority in this network. Moreover, the key management of this protocol increases the security level of the network by changing the key values in the specific period of time and also it has very low communication overhead. Furthermore, the mentioned scheme can be used in both of the unicast and multicast communications.

As it is stated in [25], a lightweight authentication methods are necessary for smart grid for two important reasons, low latency and low communication overhead. In [25], the smart meters establish a mutual authentication at first to generate a shared session keys based on the Diffie-Hellman exchange protocol. After that, by using the hash based authentication code and mentioned shared session keys, the smart meters are able to authenticate received messages in a lightweight way, thus the scheme does not contribute to high latency and exchange few signal messages during the message authentication process. Sule *et al.* [26] proposed a variable length message authentication scheme for secure communication in the smart grid. This scheme has low time for verification and provides an efficient solution to support high frequency exchange of large volume messages. Mahmood *et al.* [27] designed an elliptic curve based authentication scheme in which two users can authenticate each other and agree on a secure session key. In this protocol each user registers itself with the trusted third party. Then each registered participant can start authentication procedure with another user to initiate secure session of communication after successful authentication. Abbasinezhad *et al.* [28] found that Mahmood *et al.*'s scheme [27] does not provide the perfect forward secrecy and is vulnerable to both known session-specific temporary information attack and private keys leakage. In addition, Abbasinezhad *et al.* [28] proposed an improved scheme that eliminates the mention vulnerabilities and it is more efficient than the Mahmood *et al.*'s scheme [27].Chen *et al.* [29] found that Abbasinezhad *et al.*'s scheme suffers from the replay attack, although the adversary can not get the session key, the adversary can make this entity inaccessible to its peer entities temporarily, besides, in the first message of their scheme, there is not a signature or a timestamp, a receiver of this message can not know if this message has been tampered or altered by an adversary or not.

1.2 Research Contributions

In this paper, we evaluate a recent lightweight authentication scheme for smart grid [1] and found that it is vulnerable to KCI attack. Moreover, we show that the scheme cannot satisfy forward secrecy and privacy preserving properties [14] as important security features for authentication and key establishment in smart grid . After that, we introduce an enhanced secure authentication scheme for smart grid that eliminates the security weaknesses of Mahmood *et al.*'s scheme. In addition, we pose some formal security analysis for our scheme with AVISPA and BAN logic to show security of the proposed scheme. Finally, some security and efficiency comparisons are discussed that indicate the security and efficiency of our scheme to be utilized in smart grid.

1.3 Paper Organization

The remainder of this paper is organized as follows, some preliminaries are introduced in Section 2. A review of Mahmood *et al.*'s scheme and details of our proposed scheme are presented in Section 3 and 4, respectively. Security of the proposed scheme is analysed in Section 5. Finally, conclusion of this paper is stated in Section 6.

2 Preliminaries

In this section, we discuss the following system and threat models needed in this paper.

2.1 System model

The system model which is used in the Mahmood's scheme has four different entities, including home area network, building area network, neighborhood area network and key generation center. These four entities of the mentioned system model are defined as follows [25]:

- Home Area Network (HAN): This part consists of all smart parts of an apartment. Different smart appliances such as refrigerator, television and so on in an apartment which have their unique identity address to connect to HAN gateway. HAN gateway can communicate with BAN gateway and enables consumer to manage their on-demand requirements and their energy consumption.
- Building Area Network (BAN): Each BAN comprises number of HANs. All of the HAN gateways can communicate with control center of the smart grid only through the BAN gateways. The BAN gateway is used to monitor the power consumption and usage of HANs in its corresponding apartment.
- Neighborhood Area Network (NAN): NAN represents a particular region, for instance a city with specific number of consumers. NAN gateway is used to monitor the power consumption of this region and also manages all of the BAN gateways which are placed in its area.
- Key Generation Center (KGC): This part is responsible for generating public and private keys of all of the gateway nodes in the network. Besides that, it generates and distributes the public parameters of the network such as hash functions.

2.2 Threat model

We assume that the adversary eavesdrops and intercepts communications between HAN and BAN. Moreover, the adversary can execute the following attacks:

- Replay attack: The adversary records a valid transmission of HAN (BAN) and sends it again to BAN (HAN) for attacking proposes.
- Forward secrecy: The adversary that compromised the long term private key of HAN and BAN cannot calculate the previous session keys established by them.
- Key Compromise Impersonation (KCI) attack: If the long term private key of HAN (BAN) is compromised, the adversary can easily forge it. But, this leakage should not enable the adversary to impersonate BAN (HAN) [30].
- Privacy violation: The adversary is willing to obtain the identity of HAN and BAN for malicious purposes in smart grid [31].

2.3 Notations

The used notations of this paper are shown in Table 1.

3 Review of Mahmood et al.'s Scheme

In this section, we review a lightweight authentication scheme for smart grid communications which is proposed in [1]. This scheme has three phases including initialization, authentication and message transmission. In the following, we briefly explain these three phases.

3.1 Initialization

The KGC selects a group G of a large prime order q which satisfies CDH (Computational Diffie-Hellman) assumption. To generate asymmetric encryption key pair for each gateway node GN_j, the KGC chooses a

Table 1. Notations used in this paper

Notation	Description
HAN_{GW_i}	The smart meter gateway on home area network i
BAN_{GW_j}	The smart meter gateway on building area network j
ID_i, ID_j	The identities of HAN_{GW_i} and $BANGW_j$, respectively
s_i, s_j	The private key of HAN_{GW_i} and $BANGW_j$, respectively
P_i, P_j	The public key of HAN_{GW_i} and $BANGW_j$, respectively
$E(.), D(.)$	AES encryption and decryption
$HMAC_k(.)$	A hash-based message authentication code via a symmetric key k
$H(.)$	A collision-resistant one-way cryptographic hash function
$=?$	Checking the equality of two values
$X.Y$	X multiplies Y

random number $s_j \in Z_q^*$ as a private key for gateway node j and then computes its public key such as $P_j = g^{s_j}$ in which g is the generator of group G. After that, the public and private key pair (s_j, P_j) are sent to its corresponding node GN_j through a secure channel. Moreover, the KGC chooses a secure hash function $H(.)$ and a hash-based message authentication code which is represented by $HMAC_k$; also, it selects a unique identity for each of the gateway nodes in its network. Finally, the KGC issues identities, public keys of gateway nodes and those two hash functions to all of the gateway nodes in the network as public parameters.

3.2 Authentication

When a consumer wants to send its on-demand power list to control center, at first, an authentication process is performed between its home area network gateway node and its corresponding building area network gateway node which are represented as HAN_{GW_i} and BAN_{GW_j}, respectively. Besides that, a shared session key is computed for a symmetric cryptography between HAN_{GW_i} and BAN_{GW_j} during this process. The authentication process has three steps as follows:

1^{st} step:
HAN_{GW_i} chooses a random number $a \in Z_q^*$ and then computes three values according to $A = a(s_i + t_i)^{-1}$, $B = P_j^a$ and g^a, in which s_i, P_j and t_i represent the private key of HAN_{GW_i}, the public key of BAN_{GW_j} and time stamp recorded by HAN_{GW_i}, respectively. After that, HAN_{GW_i} uses B value as the encryption key of the AES encryption algorithm which is shown as $E(.)$ and calculates $C_i = E_B(ID_i||ID_j||B||t_i||g^a)$, in which ID_i and ID_j are the identities of HAN_{GW_i} and BAN_{GW_j}, respectively. Finally, HAN_{GW_i} sends quadruple set $< C_i, t_i, A, ID_i >$ to BAN_{GW_j}.

2^{st} step:
Upon receiving the quadruple set $< C_i, t_i, A, ID_i >$, BAN_{GW_j} checks the validity of time stamp t_i and if it is valid then computes $B = (P_i.g^{t_i})^{A.s_j}$, in which P_i and s_j represent the public key of HAN_{GW_i} and the private key of BAN_{GW_j}, respectively. After that, BAN_{GW_j} decrypts C_i according to $D_B(C_i) = (ID_i||ID_j||B||t_i||g^a)$ and then checks whether B and t_i are similar to the the values which are received in the plaintext or not. If one of the validation is failed, the BAN_{GW_j} rejects the request. Otherwise, BAN_{GW_j} chooses a random value $b \in Z_q^*$ and computes
$C_j = E_B(ID_i||ID_j||t_j||g^b||HMAC_B(ID_i||ID_j||t_j||g^b))$
in which t_j is the time stamp recorded by BAN_{GW_j}. Finally, BAN_{GW_j} sends triplex set $< C_j, t_j, ID_j >$ to HAN_{GW_i}.

3^{st} step:
After receiving triplex set $< C_j, t_j, ID_j >$, HAN_{GW_i} decrypts C_j and then checks the validation of time stamp t_j. If the time stamp is valid, HAN_{GW_i} computes $HMAC_B(ID_i||ID_j||t_j||g^b)$ and compares it with the one in the decryption in C_j. If these values are equal, BAN_{GW_j} is authenticated. At the end of this process, HAN_{GW_i} and BAN_{GW_j} calculates the shared session key according to $K_{ij} = H(ID_i||ID_j||g^{ab})$.

3.3 Message Transmission

In this phase, HAN_{GW_i} sends its on-demand request message M_i to BAN_{GW_j} in a secure channel by using AES encryption algorithm and shared session key K_{ij}. Also, HMAC algorithm is used to provide message integrity. Besides that, the time stamp t_i is used to provide replay attack resistant in this phase. Finally, HAN_{GW_i} computes

$C = E_{K_{ij}}(M_i||t_i||HMAC_{K_{ij}}(M_i))$ and sends it to BAN_{GW_j}.

Upon receiving C, BAN_{GW_j} decrypts C by using shared session key K_{ij}, validates time stamp t_i, computes $HMAC(M_i)$ and checks whether the computed $HMAC(M_i)$ is equal to the received one or not. If they are equal, BAN_{GW_j} accepts M_i and sends it to NAN_{GW_k}.

3.4 Weaknesses of Mahmood et al.'s Scheme

In this section, we find out that Mahmood *et al.*'s scheme is vulnerable to Key Compromise Impersonation (KCI) attack and it does not satisfy forward secrecy and privacy preserving properties. The details of the proposed attacks are described as follows:

- **KCI attack**: KCI vulnerability [30] is a weakness of an authenticated key agreement protocol which allows an attacker who has obtained the secret key of a client (e.g., private key of the smart meter gateway on home area network i, HAN_{GW_i}) to not just impersonate the compromised client to a server(e.g., the smart meter gateway on building area network j, BAN_{GW_j}), which is trivial, but also to impersonate a server to the compromised client. Let an adversary has obtained s_i which is the secret key of HAN_{GW_i}. It plays the role of BAN_{GW_j} as follows:
  (1) Like the protocol, HAN_{GW_i} sends the values $< C_i, t_i, A, ID_i >$ to BAN_{GW_j}.
  (2) By receiving the message, the adversary computes value B as below:
  $$B = P_j^{A(s_i+t_i)} \quad (1)$$
  Via B, it decrypts C_i, obtains ID_i, ID_j, B, t_i, g^a, selects a random number $b \in Z_q^*$ and computes ciphertext $C_j = E_B(ID_i||ID_j||t_j||g^b||HMAC_B(ID_i||ID_j||t_j||g^b))$. Finally, the adversary sends triplex set $< C_j, t_j, ID_j >$ to HAN_{GW_i}.
  (3) After receiving the message, HAN_{GW_i} decrypts C_j, verifies B and t_j and accepts the adversary as the legitimate BAN_{GW_j}.
  Thus, Mahmood *et al.*'s scheme is vulnerable to KCI attack.
  Here, we show the correctness of the value B in Equation (1).
  $$B = P_j^{A(s_i+t_i)} = P_j^{As_i}.P_j^{A.t_i} = P_i^{As_j}.g^{A.t_i.s_j} = (P_i.g^{t_i})^{A.s_j} \quad (2)$$
- **Forward secrecy:** A key agreement protocol has forward security if the long-term secret key of a participant of the key agreement protocol is compromised, the secrecy of previous session keys is not affected. Assume that an adversary obtains s_i as the long-term secret key of HAN_{GW_i} and has recorded transcripts of previous sessions of HAN_{GW_i} according to the Mahmood *et al.*'s scheme. The adversary calculates the values $a = A(s_i + t_i)$ and $B = P_j^a$. The adversary decrypts ciphertext c_j via the key B and obtains g^b. Finally, it can calculate the session key $K_{ij} = H(ID_i||ID_j||g^{ab})$. Thus, the Mahamood *et al.*'s scheme does not have forward secrecy.
- **Privacy preserving:** One of the most important requirements for smart grid is privacy preserving [14, 31] which emphasizes of the anonymity of the customers. In the Mahmood *et al.*'s scheme, identity of HAN_{GW_i} is plainly sent to BAN_{GW_j}. Thus, an eavesdropper can easily obtain the identity of HAN_{GW_i} and traces the communications of the customers.

4 The Proposed Scheme

Like Mahmood *et al.*'s scheme, our scheme contains three phases initialization, authentication and message transmission. The initialization phase is same as one in Mahmood *et al.*'s scheme but $q-1$ has a large prime factor p. We describe the authentication and message transmission phases of our scheme as follows. In addition, details of our scheme is shown in Figure 2.

4.1 Authentication

This phase is executed between HAN_{GW_i} and BAN_{GW_j} in order that authenticate each other and agree on a symmetric key for the secure message transmission. The authentication is done via the following three steps.

1^{st} step:
HAN_{GW_i} selects a random number $a \in Z_p^*$ and calculates $A = g^a$, $TID_i = ID_i \oplus H(P_j^a)$ and $V = a + s_i H(ID_i||ID_j||A||t_i)\ modp$ in which s_i is the private key of HAN_{GW_i}, P_j is the public key of BAN_{GW_j}, t_i is a time stamp obtained by HAN_{GW_i} and ID_i and ID_j are the identities of HAN_{GW_i} and BAN_{GW_j}, respectively. Finally, HAN_{GW_i} sends $< t_i, A, TID_i, V >$ to BAN_{GW_j}.

2^{nd} step:
After receiving the message, BAN_{GW_j} checks the validity of time stamp t_i and if it is true then calculates $ID_i = TID_i \oplus H(A^{s_j})$. BAN_{GW_j} checks that $A = g^V P_i^{-H(ID_i||ID_j||A||t_i)}$ is hold, where P_i is the public key of HAN_{GW_i}. If the validation is failed, the BAN_{GW_j} rejects the request. Other-

wise, BAN_{GW_j} selects a random number $b \in Z_p^*$ and calculates $B = g^b$, $L = (A.P_i)^{s_j}$ and $C_j = HMAC_L(ID_j||ID_i||A||B||t_j)$ in which t_j is the time stamp recorded by BAN_{GW_j}. Finally, BAN_{GW_j} sends $< t_j, B, C_j >$ to HAN_{GW_i}.

3^{rd} step:
Upon receiving the message, HAN_{GW_i} checks the validity of time stamp t_j and if it is true then computes $L = P_j^{(a+s_i)}$. HAN_{GW_i} checks that $C_j = HMAC_L(ID_j||ID_i||A||B||t_j)$ is hold. If it is, HAN_{GW_i} accepts BAN_{GW_j} and calculates the session key as below:

$$K_{ij} = H(ID_i||ID_j||A||B||(g^b)^a) \tag{3}$$

In like manner, BAN_{GW_j} computes the session key as follows:

$$K_{ij} = H(ID_i||ID_j||A||B||(g^a)^b) \tag{4}$$

4.2 Message Transmission

After constructing the secure common secret key K_{ij}, HAN_{GW_i} can securely send the demand request message M_i which contains the electricity requirements of the smart appliances for certain period of time, to BAN_{GW_j}. For this issue, HAN_{GW_i} utilizes AES algorithm via the key K_{ij}, obtains a time stamp t_m and transmits $t_m, C = E_{K_{ij}}(ID_i||ID_j||t_m||M_i)$ to BAN_{GW_j}. After receiving the message, BAN_{GW_j} checks t_m and if it is valid then decrypts C and obtains ID_i, ID_j, t_m, and M_i. BAN_{GW_j} verifies the correctness of ID_i, ID_j, t_m and if they are true values, BAN_{GW_j} accepts M_i as the demand request message of HAN_{GW_i}.

5 Security Analysis

In this section, we evaluate the security properties and introduce a formal analysis of our scheme. Then, we compare the proposed scheme with some related schemes in terms of security and efficiency.

5.1 Security Properties

- **Mutual authentication:** In our scheme, HAN_{GW_i} and BAN_{GW_j} calculates common value B which only can be computed by them. In 2^{st} step, BAN_{GW_j} decrypts C_i and checks correctness of ID_i, ID_j and t_i. If these values are true, BAN_{GW_j} authenticates HAN_{GW_i}. Similarly, HAN_{GW_i} decrypts C_j and checks whether ID_i, ID_j and t_j are correct values ,and if so, HAN_{GW_i} authenticates BAN_{GW_j}.Thus, our scheme provides mutual authentication property.
- **Resilient to replay attack:** Due to the time stamps which are used in the flows, all transmitted messages are fresh. Then, our scheme is resilience to replay attack.
- **Forward secrecy:** In our scheme, the session key is calculated from the fresh value g^{ab} and this value is independent from the long term secret keys s_i and s_j. Hence, if the adversary obtains secret keys of BAN_{GW_j} and HAN_{GW_i}, it cannot compute the previous session keys. Thus, our scheme satisfies the forward secrecy property.
- **KCI attack resiliency:** Let the adversary has obtained the secret key s_i of HAN_{GW_i}. The adversary needs to compute $L = (A.P_i)^{s_j} = A^{s_j}.P_j^{s_i}$ to impersonate BAN_{GW_j}. But it cannot calculate L because of the term A^{s_j} , and hence the proposed scheme is immune to KCI attack. Moreover, the adversary that obtains s_j cannot impersonate HAN_{GW_i} to BAN_{GW_j} because it is unable to compute a valid value V without knowing the secret key s_i .
- **Privacy preserving:** In 1^{st} step of our protocol, HAN_{GW_i} sends $TID_i = ID_i \oplus H(P_j^a)$ to BAN_{GW_j}. TID_i does not reveal any information about ID_i to an eavesdropper and this preserves anonymity of the HAN_{GW_i}. Thus, the proposed scheme provides privacy preserving property.

  Finally, security properties of our scheme is compared with security features of related schemes. The comparison is shown in Table 2. It indicates that the proposed scheme has more security features as compared to Mahmood *et al.*'s scheme.

5.2 Formal Security Verification Using AVISPA Tool: Simulation Study

In this section, we evaluate the proposed scheme for the formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [32]. We provide the implementation details of the proposed scheme in the High-Level Protocol Specification Language (HLPSL) [33] and then the simulation results. It is worth noticing that AVISPA only captures replay and man-in-the-middle attacks against an attacker for any security protocol.

5.2.1 Overview of AVISPA

AVISPA is an automated validation tool with a high-level language specification for the security sensitive applications and protocols [32]. In recent years, AVISPA becomes a popular and powerful tool for the formal security verification [32, 34–41]. The

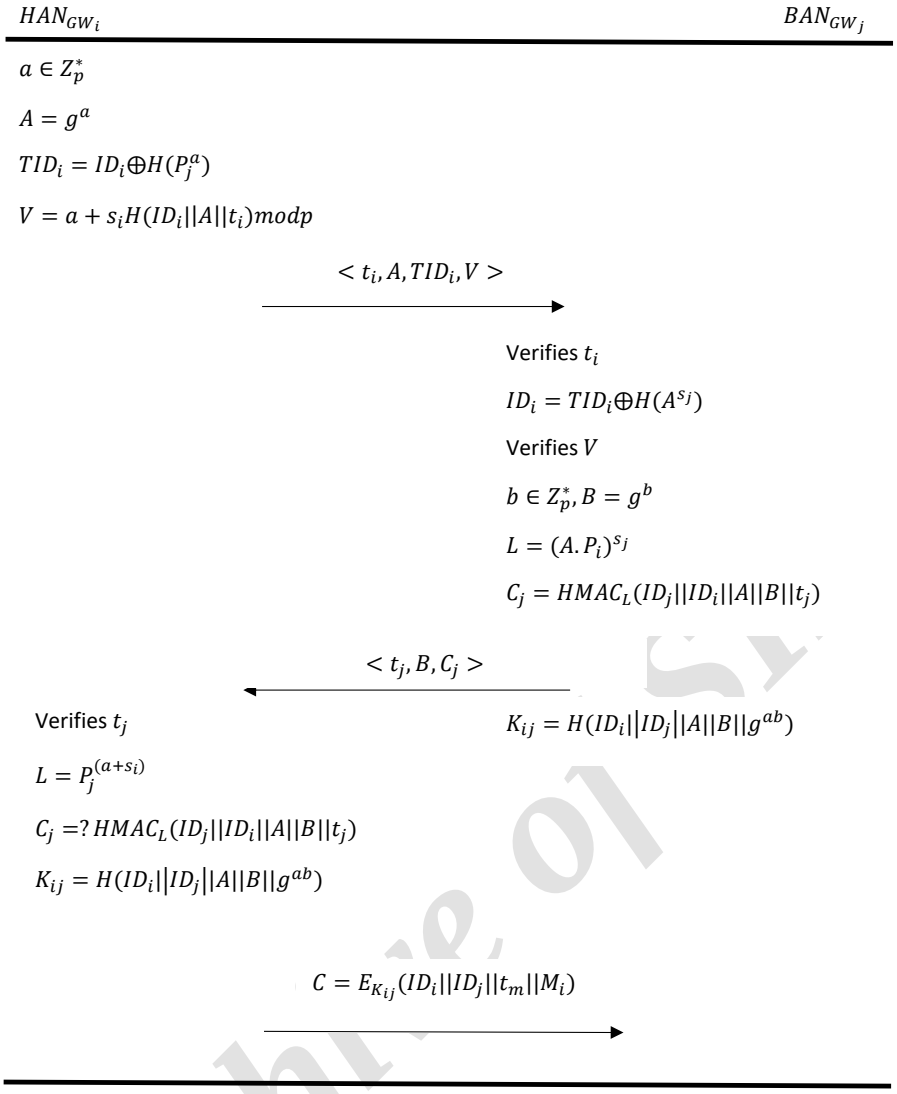

Figure 2. The proposed scheme

Table 2. Security comparison

Scheme	Our	Mahmood *et al.* [1]	Fouda *et al.* [25]	Sule *et al.* [26]	Mahmood *et al.*[27]	Abbasinezhad *et al.* [28]	Chen *et al.* [29]
Mutual authentication	YES	YES	YES	YES	YES	YES	YES
Resilient to reply attack	YES	YES	YES	YES	YES	NO	YES
Forward secrecy	YES	NO	YES	YES	NO	NO	YES
KCI attack resiliency	YES	NO	YES	YES	YES	YES	YES
Privacy-preservation	YES	NO	YES	YES	NO	NO	NO

architecture of the AVISPA tool is shown in Figure 3. AVISPA provides various automatic analysis techniques through its four back-ends: 1) On-the-fly Model-Checker (OFMC), 2) Constraint Logic based Attack Searcher (CL-AtSe), 3) SAT-based Model-Checker (SATMC) and 4) Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP). More detailed descriptions on these back-ends can be found in [32].

The security protocols which are to be analyzed for their security part by AVISPA tool need to be specified in HLPSL (High Level Protocols Specification Language) [33]. HLPSL is a role based language and contains the following roles [32, 33]:

- Basic roles: These roles, in general, represent different participating entities in the protocol.
- Composition roles: These roles represent different scenarios involving basic roles.

In HLPSL, an intruder is represented as one of the

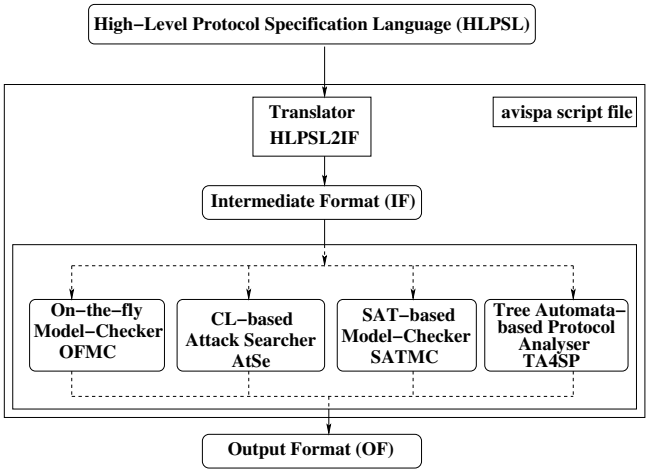

Figure 3. Architecture of AVISPA [32]

basic legitimate roles and is always represented by i. The HLPSL specification of the protocol is translated to its intermediate format (IF) using the HLPSL2IF translator, and then IF is converted to output format (OF) by one of the four back-ends. The OF typically has the following sections [33]:

- SUMMARY: It defines whether the tested protocol is safe, unsafe, or whether the analysis is inconclusive.
- DETAILS: It states a detailed explanation of why the tested protocol is concluded as safe, or under what conditions the test application or protocol is exploitable using an attack, or why the analysis is inconclusive.
- PROTOCOL: It defines the HLPSL specification of the target protocol in intermediate form.
- GOAL: The goal of the analysis which is being performed by AVISPA using HLPSL specification.
- BACKEND: The name of the back-end that is used for the analysis, that is, one of OFMC, CL-AtSe, SATMC and TA4SP.
- Finally, the trace of a possible vulnerability to the target protocol, if any, along with some useful statistics and relevant comments.

5.2.2 Specifying the Protocol

We have implemented the proposed scheme for the authentication and message transmission phases. The HLPSL specification for the role of HAN_{GW_i} is given in Figure 4 and the Appendix.

5.2.3 Analysis of Simulation Results

The proposed scheme is simulated using OFMC and CL-AtSe backends under the SPAN, the Security Protocol ANimator for AVISPA tool [42]. It is worth noticing that the proposed scheme uses the bitwise

```
role han_gwi(HANgwi, BANgwj: agent,
        H: hash_func,
        Snd, Rcv: channel(dy))
played_by HANgwi
def=
 local State: nat,
      A, A1, TIDi, V, IDi, Ti, P, G, Si, Sj, Pj: text,
      F, HMAC: hash_func,
      Kij, Tj, IDj, B, Mi, Tm, C: text
 const sp1, sp2, sp3, han_ban_a, han_ban_ti, han_ban_tm,
      ban_han_b, ban_han_tj: protocol_id
% Initialize state, State to 0
init State := 0
transition
%%% Authentication phase
1. State = 0 ∧ Rcv(start) =|>
%%% A is random number and Ti is current timestamp
 State' := 1 ∧ A' := new() ∧ Ti' := new()
         ∧ A1' := exp(G, A')
%%% Si is private key of HANgwi and Pj is public key of BANgwj
%%% Sj is private key of BANgwj and Pi is public key of HANgwi
         ∧ TIDi' := xor(IDi, H(exp(exp(G, Sj), A')))
         ∧ V' := F(A'.Si.H(IDi.A1'.Ti').P)
         ∧ secret({IDi, IDj}, sp1, {HANgwi, BANgwj})
         ∧ secret(Si, sp2, {HANgwi})
%%% Send message <ti, A, TIDi, V> to BANgwj via public channel
         ∧ Snd(Ti'.A1'.TIDi'.V')
% HANgwi has freshly generated the random number a for the BANgwj
         ∧ witness (HANgwi, BANgwj, han_ban_a, A')
% HANgwi has freshly generated the current timestamp ti for the BANgwj
         ∧ witness (HANgwi, BANgwj, han_ban_ti, Ti')
%%% Receive message <tj, B, Cj> from BANgwj via open channel
2.  State = 1 ∧ Rcv(Tj'.exp(G, B').HMAC(exp(F(exp(G, A').exp(G, Si)),
            Sj).IDj.IDi.exp(G, A').exp(G, B').Tj')) =|>
 State' := 3 ∧ secret(Sj, sp3, {BANgwj})
%%% Mi is the demand request message of HANgwi
%%% Tm is the current timestamp
         ∧ Mi' := new() ∧ Tm' := new()
%%% Kij is the session key between HANgwi and BANgwj
         ∧ Kij' := H(IDi.IDj.exp(G, A').exp(G, B').
                   exp(exp(G, B'), A'))
         ∧ C' := {IDi.IDj.Tm'.Mi'}_Kij'
%%% Send message <tm, C> to BANgwj via open channel
         ∧ Snd(Tm'.C')
% HANgwi has freshly generated the current timestamp tm for the BANgwj
         ∧ witness (HANgwi, BANgwj, han_ban_tm, Tm')
% HANgwi's acceptance of b and tj generated for HANgwi by BANgwj
         ∧ request(BANgwj, HANgwi, ban_han_b, B')
         ∧ request(BANgwj, HANgwi, ban_han_tj, Tj')
end role
```

Figure 4. HLPSL specification for the role of HAN_{GW_i}

XOR operations. Currently, other backends, namely SATMC and TA4SP do not support this feature of implementing XOR operations in the roles. As a result, the simulation results of the proposed scheme using SATMC and TA4SP backends come as "inconclusive", and hence, we have ignored these results from this paper.

Three verifications needed for the proposed scheme in both the cases: 1) executability checking on non-trivial HLPSL specifications; 2) replay attack checking; and 3) Dolev-Yao model checking. The executability check is necessary to ensure that the protocol will reach to a state where a possible attack can happen, during the run of the protocol. From Figure 4 and Figure 5, it is shown that the proposed scheme is properly translated to HLPSL specification and it meets the design goals by ensuring the executability. The proposed scheme is also simulated for the execution tests and a bounded number of sessions model

```
role ban_gwj(HANgwi, BANgwj: agent,
        H: hash_func,
        Snd, Rcv: channel(dy))
played_by BANgwj
def=
 local State: nat,
      A, A1, TIDi, V, IDi, Ti, P, G, Si, Sj, Pi, Pj: text,
      F, HMAC: hash_func,
      Tj, IDj, B, B1, L, Cj, Tm, Mi: text
 const sp1, sp2, sp3, han_ban_a, han_ban_ti, han_ban_tm,
      ban_han_b, ban_han_tj : protocol_id
% Initialize state, State to 0
init State := 0
transition
%%% Authentication phase
%%% Receive message <ti, A, TIDi, V> from HANgwi via public channel
1. State = 0 /\ Rcv(Ti'.exp(G, A').xor(IDi, H(exp(exp(G, Sj), A'))).
                F(A'.Si.H(IDi.exp(G, A').Ti').P))  =|>
 State' := 2 /\ secret({IDi, IDj}, sp1, {HANgwi, BANgwj})
          /\ secret(Si, sp2, {HANgwi})
          /\ secret(Sj, sp3, {BANgwj})
%%% B is random number and Tj is current timestamp
          /\ B' := new() /\ Tj' := new()
          /\ B1' := exp(G, B')
          /\ L' := exp(F(exp(G, A').exp(G, Si)), Sj)
          /\ Cj' := HMAC(L'.IDj.IDi.exp(G, A').B1'.Tj')
%%% Send message <tj, B, Cj> to HANgwi via open channel
          /\ Snd(Tj'.B1'.Cj')
% BANgwj has freshly generated the random number b for the HANgwi
          /\ witness (BANgwj, HANgwi, ban_han_b, B')
% BANgwj has freshly generated the current timestamp tj for the HANgwi
          /\ witness (BANgwj, HANgwi, ban_han_tj, Tj')
%%% Receive message <tm, C> from HANgwi via open channel
2. State = 2 /\ Rcv(Tm'.{IDi.IDj.Tm'.Mi'}_(H(IDi.IDj.exp(G, A').
                exp(G, B').exp(exp(G, B'), A')))) =|>
% BANgwj's acceptance of a, ti and tm generated for BANgwj by HANgwi
 State' := 4 /\ request(HANgwi, BANgwj,  han_ban_a, A')
          /\ request(HANgwi, BANgwj,  han_ban_ti, Ti')
          /\ request(HANgwi, BANgwj,  han_ban_tm, Tm')
end role
```

Figure 5. HLPSL specification for the role of BAN_{GW_j}

```
role session(HANgwi, BANgwj: agent, H: hash_func)
def=
 local Snd1, Rcv1, Snd2, Rcv2: channel (dy)
 composition
    han_gwi(HANgwi, BANgwj, H, Snd1, Rcv1)
 /\ ban_gwj(HANgwi, BANgwj, H, Snd2, Rcv2)
end role

role environment()
def=
 const hangwi, bangwj: agent,
    h, f, hmac: hash_func,
    ti, tj, tm: text,
    sp1, sp2, sp3, han_ban_a, han_ban_ti,
    han_ban_tm, ban_han_b, ban_han_tj: protocol_id
intruder_knowledge = {h, f, hmac, ti, tj, tm}
%%% i is the intruder
composition
  session(hangwi, bangwj, h)
/\ session(i, bangwj, h)
/\ session(hangwi, i, h)
end role

goal
%%% Confidentiality (privacy)
secrecy_of sp1, sp2, sp3
%%% Authentication
authentication_on han_ban_a, han_ban_ti
authentication_on han_ban_tm
authentication_on ban_han_b, ban_han_tj
end goal
environment()
```

Figure 6. HLPSL specification for the role of session, goal and environment

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\auth−smartgrid.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.04s
  visitedNodes: 16 nodes
  depth: 4 plies
```

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\auth−smartgrid.if
GOAL
  As Specified

BACKEND
  CL−AtSe

STATISTICS
  Analysed   : 15 states
  Reachable  : 15 states
  Translation: 0.00 seconds
  Computation: 0.02 seconds
```

Figure 7. The results of the analysis using OFMC and CL-AtSe backends

checking. To check the replay attack on the proposed protocol, both the backends (OFMC and CL-AtSe) verify if the legitimate agents can execute the specified protocol by performing a search of a passive intruder. These back-ends then supply the intruder (i) about the knowledge of some normal sessions between the valid agents. On the other hand, both OFMC and CL-AtSe backends check if any man-in-the-middle attack possible by i for the Dolev-Yao model checking.

The simulation results for both the OFMC and L-AtSe backends are reported in Figure 7. OFMC backend takes 0.04 seconds search time, while it visits 16 nodes with a depth of 4 plies, whereas CL-AtSe backend analyzes 15 states and it takes 0.02 seconds computation time, and all 15 states are reachable. Therefore, all verifications, such as executability checking on non-trivial HLPSL specifications, replay attack checking and Dolev-Yao model checking are satisfied in the proposed scheme. As a result, the proposed scheme becomes safe against both replay & man-in-the-middle attacks.

5.3 Mutual Authentication Based on BAN Logic

In this section, we present the formal proof by BAN logic [43]. We assume HAN_{GW_i} and BAN_{GW_j} are legal entities and they mutually authenticate each other in our scheme. The notions are given in Table 3.

Ban Rules: There are five rules in the BAN logic:

(1) *Message meaning:*

Table 3. The formal notations in the BAN logic [43]

Notation	Description
$P\|\equiv X$	P believes X, or P would be entitled to believe X
$P \triangleleft X$	P sees X. A party has sent a message containing X to P who can read and repeat X.
$P\|\sim X$	P once said X. P sent a message including the statement X before, and P believed X when he sent the message.
$P\|\Rightarrow X$	P has jurisdiction over X. P is an authority on X and should be trusted on this matter.
$\#(X)$	X is fresh, and X has not been sent in a message at any time before the current run of the protocol.
$P \overset{X}{\Longleftrightarrow} P'$	X is a secret known only to P and P', and trusted by them. Only P and P' may use X to prove their identities to each other.
(X,Y)	Formula X or Y is a part of formula (X,Y)
$< X >_K$	Formula X is encrypted under the key K
$\{X\}_Y$	X is combined with the formula Y. It means that Y is a secret and that its presence prove the identity of whoever utters $\{X\}_Y$

$$\frac{P|\equiv P \overset{K}{\Longleftrightarrow} Q, P \triangleleft \{X\}_K}{P|\equiv Q|\sim X}$$

and

$$\frac{P|\equiv P \overset{Y}{\rightleftharpoons} Q, P \triangleleft < X >_Y}{P|\equiv Q|\sim X}$$

(2) *Nonce-verification:*

$$\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

(3) *Jurisdiction:*

$$\frac{P|\equiv Q \Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$$

(4) *Freshness-conjuncatenation rule:*

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$$

(5) *Session key rule [44]:*

$$\frac{P|\equiv \#(X), P|\equiv Q|\equiv \{X\}_K}{P|\equiv P \overset{K}{\Longleftrightarrow} Q}$$

Goals: In accordance with BAN logic procedures, the proposed scheme should satisfy following goals:

Goal 1: $HAN_{GW_i}|\equiv (HAN_{GW_i} \overset{SK}{\longleftrightarrow} BAN_{GW_j})$

Goal 2: $HAN_{GW_i}|\equiv BAN_{GW_j}|\equiv (HAN_{GW_i} \overset{SK}{\longleftrightarrow} BAN_{GW_j})$

Goal 3: $BAN_{GW_j}|\equiv (BAN_{GW_j} \overset{SK}{\longleftrightarrow} HAN_{GW_i})$

Goal 4: $BAN_{GW_j}|\equiv HAN_{GW_i}|\equiv (BAN_{GW_j} \overset{SK}{\longleftrightarrow} HAN_{GW_i})$

Idealized form: The proposed protocol transformed into idealized form as follows:

Message 1: $HAN_{GW_i} \rightarrow BAN_{GW_j} : BAN_{GW_j} \triangleleft t_i, BAN_{GW_j} \triangleleft A, BAN_{GW_j} \triangleleft TID_i, BAN_{GW_j} \triangleleft V :< a >_{h(ID_i)}$

Message 2: $BAN_{GW_i} \rightarrow HAN_{GW_j} : HAN_{GW_j} \triangleleft t_j, HAN_{GW_j} \triangleleft B, HAN_{GW_j} \triangleleft C_j :< b >_L$

Message 3: $HAN_{GW_i} \rightarrow BAN_{GW_j} : BAN_{GW_j} \triangleleft C :< M_i >_{k_{ij}}$

Hypotheses: The following six assumptions are considered:

A1: $HAN_{GW_i}|\equiv \#\{a\}$

A2: $BAN_{GW_j}|\equiv \#\{b\}$

A3: $HAN_{GW_i}|\equiv HAN_{GW_i} \overset{h(ID_i)}{\longleftrightarrow} BAN_{GW_j}$

A4: $BAN_{GW_j}|\equiv BAN_{GW_j} \overset{L}{\longleftrightarrow} HAN_{GW_i}$

A5:$BAN_{GW_j}|\equiv HAN_{GW_i} \Rightarrow a$

A6:$HAN_{GW_i}|\equiv BAN_{GW_j} \Rightarrow b$

We verify accuracy of the proposed scheme as follows:

- From Message 1, we obtain
  S1: $BAN_{GW_j} \triangleleft t_i, A, TID_i, V :< a >_{h(ID_i)}$
- Using Message Meaning Rule, A3 and S1, we obtain
  S2: $BAN_{GW_j}|\equiv HAN_{GW_i}|\sim a$
- Using Nonce Verification Rule, A2 and S2, we procure
  S3: $BAN_{GW_j}|\equiv HAN_{GW_i}|\equiv a$
- Using Jurisdiction Rule, A5 and S3, we can obtain
  S4: $BAN_{GW_j}|\equiv a$
- Using Session key rule, S3 and A2, we get
  S5 (**Goal 3**): $BAN_{GW_j}|\equiv (BAN_{GW_j} \overset{SK}{\longleftrightarrow} HAN_{GW_i})$

Table 4. Communication costs comparison

Scheme	Step 1 (bytes)	Step 2 (bytes)	Step 3 (bytes)	Total no. of bytes)
Fouda *et al.* [25]	160 $2L_{ID}+L_E$	288 $2L_{ID}+2L_E$	164 $L_T+L_H+L_E$	612
Sule *et al.* [26]	160 $2L_{ID}+L_E$	288 $2L_{ID}+2L_E$	164 $L_T+L_H+L_E$	612
Mahmood *et al.* [27]	92 $3L_S+L_{ID}+L_T$	92 $3L_S+L_{ID}+L_T$	Nil	184
Abbasinezhad *et al.* [28]	56 $2L_S+L_{ID}$	76 $2L_S+L_H+L_{ID}$	36 $L_{ID}+L_H$	168
Chen *et al.* [29]	92 $3L_S+L_{ID}+L_T$	76 $2L_S+L_{ID}+L_H$	Nil	168
Mahmood *et al.* [1]	356 $3L_{ID}+2L_E+2L_T+L_p$	228 $3L_{ID}+L_E+2L_T+L_H$	Nil	584
Our	184 $L_T+L_E+L_H+L_S$	164 $L_T+L_E+L_H$	Nil	348

Table 5. Computation costs comparison

Scheme	HAN_{GW_i}	BAN_{GW_j}
Fouda *et al.* [25]	$4T_M+T_H$	$5T_M+T_H$
Sule *et al.* [26]	$4T_M+T_{MAC}$	$4T_M+T_{MAC}$
Mahmood *et al.* [27]	$5T_{EC}+4T_H$	$5T_{EC}+4T_H$
Abbasinezhad *et al.* [28]	$4T_{EC}+4T_H$	$4T_{EC}+4T_H$
Chen *et al.* [29]	$T_P+3T_{EC}+4T_H$	$3T_P+3T_{EC}+4T_H$
Mahmood *et al.* [1]	$3T_M+2T_S+T_H+T_{MAC}$	$3T_M+2T_S+T_H+T_{MAC}$
Our	$4T_M+3T_H+T_{MAC}$	$6T_M+3T_H+T_{MAC}$

- From Nonce Verification Rule, S5 and A2, we get
  S6 (**Goal 4**): $BAN_{GW_j}|\equiv HAN_{GW_i}|\equiv (BAN_{GW_j} \overset{SK}{\longleftrightarrow} HAN_{GW_i})$
- From Message 2, we get
  S7: $HAN_{GW_i} \triangleleft t_j, B :< b >_L$
- Using Message Meaning Rule, S7 and A4, we can get
  S8: $HAN_{GW_i}|\equiv BAN_{GW_j}|\sim b$
- Using S8, A1 and Nonce Verification Rule, we get
  S9: $HAN_{GW_i}|\equiv BAN_{GW_j}|\equiv b$
- Using Jurisdiction Rule, A6 and S9, we can obtain
  S10: $HAN_{GW_i}|\equiv b$
- Using Session key rule, S9 and A1, we obtain
  S11 (**Goal 1**): $HAN_{GW_i}|\equiv (HAN_{GW_i} \overset{SK}{\longleftrightarrow} BAN_{GW_j})$
- From Nonce Verification Rule, S11 and A1, we get
  S12 (**Goal 2**): $HAN_{GW_i}|\equiv BAN_{GW_j}|\equiv (HAN_{GW_i} \overset{SK}{\longleftrightarrow} BAN_{GW_j})$

As all the four goals are achieved, it signifies that the session key is established between the communicating parties in our scheme.

5.4 Performance Analysis

In this section, we compare our scheme with some related schemes in terms of security and efficiency. Table 4 compares the communication cost in which the time stamp is considered 16 bytes (L_T), RSA encryption (modular exponentiation) size is 128 bytes (L_E), scalar multiplication 20 bytes (L_S), ID is 16

bytes (L_{ID}), p and $HMAC$ are 20 bytes (L_p and L_H, respectively) [1]. This comparison indicates that our scheme is about 59% more efficient than Mahmood *et al.*'s scheme in term of communication overhead.

In addition, Table 5 compares the computation cost in which the following notations are used:

- T_M: The time for RSA encryption/decryption or modular exponentiation
- T_S: Time for symmetric encryption/decryption
- T_H: Time for hash operation
- T_{MAC}: Time for HMAC.
- T_{EC}: Time for scalar multiplication.
- T_P: Time for pairing

The computation cost comparison indicates that the cost of our scheme is analogous Mahmood *et al.*'s scheme on the side of HAN_{GW_i}. Our scheme has three modular exponentiations more than Mahmood *et al.*'s scheme in the BAN_{GW_j} which is admissible cost for enhanced security features.

6 Conclusion

In this paper, we evaluated a lightweight authentication scheme for smart grid proposed by Mahmood *et al.* We pointed out their scheme is vulnerable to KCI attack and it also lacks forward secrecy and privacy preserving properties. Then, we suggested an enhanced authentication scheme for smart grid environment that provides important security features such as mutual authentication, replay and KCI attacks resiliency, forward secrecy and privacy-preservation. We carried out the formal security analysis using the BAN logic proof and also the formal security verification using the AVISPA software tool. The results ensure the security of the proposed scheme. In addition, the comparative study of our scheme with other relevant schemes reveals that our scheme performs well as compared to other techniques in terms of security and functionality features, and communication and computational costs. Hence, our scheme is efficient to be utilized in smart grid environment as compared to other existing schemes.

References

[1] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad. A lightweight message authentication scheme for smart grid communications in power sector. *Computers & Electrical Engineering*, 52:114–124, 2016.

[2] Daniel M Kammen. The rise of renewable energy. *Scientific American*, 295(3):84–93, 2006.

[3] W. Wang and Z. Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[4] J. R. Minkel. The 2003 northeast blackout–five years later. *Scientific American*, 13, 2008.

[5] S. Rohjans, M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, and T. Weidelt. Survey of smart grid standardization studies and recommendations. In *ernational conference on Smart Grid Communications (SmartGridComm)*, pages 583–588. IEEE, 2010.

[6] D. Gan, F. Liu, L. Du, and Y. Liu. Research and implementation of on-line monitoring techniques for high voltage equipments in smart grid. In *International Conference on High Voltage Engineering and Application (ICHVE)*, pages 236–239. IEEE, 2010.

[7] H. Li, L. Lu, R.and Zhou, B. Yang, and X. Shen. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Systems Journal*, 8(2):655–663, 2014.

[8] NIST Framework. Roadmap for smart grid interoperability standards, release 2.0 (2012). *Reproduced with permission of the copyright owner. Further reproduction prohibited without permission*, 2012.

[9] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. P. Chen. A survey of communication/networking in smart grids. *Future Generation Computer Systems*, 28(2):391–404, 2012.

[10] Sandhya Armoogum and Vandana Bassoo. Privacy of energy consumption data of a household in a smart grid. In *Smart Power Distribution Systems*, pages 163–177. Elsevier, 2019.

[11] Rafał Leszczyna. Standards on cyber security assessment of smart grid. *International Journal of Critical Infrastructure Protection*, 22:70–89, 2018.

[12] Kenneth Kimani, Vitalice Oduol, and Kibet Langat. Cyber security challenges for iot-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25:36–49, 2019.

[13] Y. Xiao. *Security and privacy in smart grids*. CRC Press, 2013.

[14] *Introduction to NISTIR 7628 guidelines for smart grid cyber security*. 2010. Grid, NIST Smart Guideline.

[15] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung. Network security management and authentication of actions for smart grids operations. In *Electrical Power Conference (EPC)*, pages 31–36. IEEE, 2007.

[16] R. Merkle. Protocols for public key cryptosystems. In *Proc. IEEE Symp.Security and Privacy*, pages 122–134. IEEE, 1980.

[17] R. C. Merkle. A certified digital signature. In *Conference on the Theory and Application of Cryptology*, pages 218–238. Springer, 1989.

[18] D. Hankerson, A. J. Menezes, and S. Vanstone. *Guide to elliptic curve cryptography*. Springer

Science & Business Media, 2006.

[19] M. Joye and G. Neven. *Identity-based cryptography*, volume 2. IOS press, 2009.

[20] F. Bao, R. H. Deng, and H. Zhu. Variations of diffie-hellman problem. In *International Conference on Information and Communications Security*, pages 301–312. Springer, 2003.

[21] M. C. Muñoz, M. Moh, and T. S. Moh. Improving smart grid authentication using merkle trees. In *20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, pages 793–798. IEEE, 2014.

[22] Q. Li and G. Cao. Multicast authentication in the smart grid with one-time signature. *IEEE Transactions on Smart Grid*, 2(4):686–696, 2011.

[23] L. Zhang, S. Tang, Y. Jiang, and Z. Ma. Robust and efficient authentication protocol based on elliptic curve cryptography for smart grids. In *International Conference on and IEEE Cyber, Physical and Social Computing*, pages 2089–2093. IEEE, 2013.

[24] H. Nicanfar, P. Jokar, and V. C. Leung. Smart grid authentication and key management for unicast and multicast communications. In *Proc. Innovative Smart Grid Technologies Asia (ISGT)*, pages 1–8. IEEE, 2011.

[25] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen. A lightweight message authentication scheme for smart grid communications. *IEEE Transactions on Smart Grid*, 2(4):675–685, 2011.

[26] R. Sule, R. S. Katti, and R. G. Kavasseri. A variable length fast message authentication code for secure communication in smart grids. In *Power and Energy Society General Meeting*, pages 1–6. IEEE, 2012.

[27] Khalid Mahmood, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Kumari, Xiong Li, and Arun Kumar Sangaiah. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81:557–565, 2018.

[28] Dariush Abbasinezhad-Mood and Morteza Nikooghadam. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems*, 84:47–57, 2018.

[29] Yuwen Chen, José-Fernán Martínez, Pedro Castillejo, and Lourdes López. A bilinear map pairing based authentication scheme for smart grid communications: Pauth. *IEEE Access*, 7:22633–22643, 2019.

[30] M. Bayat and M. R. Aref. An attribute based key agreement protocol resilient to kci attack. *International Journal of Electronics and Information Engineering*, 2(1):10–20, 2015.

[31] M. Bayat, H. R. Arkian, and M. R. Aref. A revocable attribute based data sharing scheme resilient to dos attacks in smart grid. *Wireless Networks*, 21(3):871–881, 2015.

[32] AVISPA. Automated Validation of Internet Security Protocols and Applications, 2018. http://www.avispa-project.org/. Accessed on April 2018.

[33] D. von Oheimb. The high-level protocol specification language hlpsl developed in the eu project avispa. In *Proceedings of 3rd APPSEM II (Applied Semantics II) Workshop (APPSEM'05)*, pages 1–17, Frauenchiemsee, Germany, 2005.

[34] S. Chatterjee and A. K. Das. An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. *Security and Communication Networks*, 8(9):1752–1771, 2015.

[35] A. K. Das. A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. *Wireless Personal Communications*, 82(3):1377–1404, 2015.

[36] A. K. Das. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*, 9(1):223–244, 2016.

[37] A. K. Das. A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. *International Journal of Communication Systems*, 30(1):1–25, 2017.

[38] C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang. An novel three-party authenticated key exchange protocol using one-time key. *Journal of Network and Computer Applications*, 36(1):498–503, 2013.

[39] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues. Cloud Centric Authentication for Wearable Healthcare Monitoring System. *IEEE Transactions on Dependable and Secure Computing*, 2018. DOI: 10.1109/TDSC.2018.2828306.

[40] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems. *Future Generation Computer Systems*, pages –, 2018. DOI: 10.1016/j.future.2018.04.019.

[41] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo. Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. *IEEE Transactions on Dependable and Secure Computing*, 2017. DOI: 10.1109/TDSC.2017.2764083.

[42] AVISPA. SPAN: Security Protocol ANimator for

AVISPA, 2018. http://www.avispa-project.org/. Accessed on April 2018.
[43] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, 1990.
[44] AM Mathuria, Reihaneh Safavi-Naini, and PR Nickolas. On the automation of gny logic. *Australian Computer Science Communications*, 17:370–379, 1995.

Majid Bayat is an assistant professor of Computer Engineering of Shahed University, Tehran, Iran. His research interests include smart grid and IoT security.

Zahra Zare Jousheghani received M.Sc. degree in communication systems from the Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran. Her research interests include cryptography and network security. author.

Ashok Kumar Das received Ph.D. degree in computer science and engineering, M.Tech. degree in computer science, and M.Sc. degree in mathematics all from IIT Kharagpur, India. He is currently an Associate Professor with the International Institute of Information Technology, Hyderabad, India. He has published more than 160 papers in international journals and conferences in the field of cryptography and network security.

Pitam Singh received his M.Sc. (Mathematics) and M.Phil. (Mathematics) from Department of Mathematics, Chaudhary Charan Singh University, Campus, Meerut, UP, India. He received his Ph.D. from the Department of Mathematics, Motilal Nehru National Institute of Technology Allahabad, India. Currently, he is an Associate Professor in the Department of Mathematics, Motilal Nehru National Institute of Technology Allahabad, India. He has published more than 20 International Journals of Repute. His research interest includes Optimization theory, Fuzzy Sets and Systems, GIS and Remote Sensing and its Applications.

Saru Kumari is currently an Assistant Professor with the Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India. She received her Ph.D. degree in Mathematics in 2012 from CCS University, Meerut, UP, India. She has published more than 115 research papers in reputed International journals and conferences, including 97 publications in SCI-Indexed Journals. She is on the Editorial Board of KSII Transactions on Internet and Information Systems (SCI-E), published from Taiwan. She is also serving as Associate Editor on Security and Privacy, Wiley. She served as Guest Editor of the Special Issue BBig-data and IoT in e-Healthcare^ for Computers and Electrical Engineering, Elsevier (SCI-E), Elsevier. She is Technical Program Committee Member for more than a dozen of International conferences. She is a reviewer of more than a dozen of reputed Journals including SCI-Indexed Journals of IEEE, Elsevier, Springer, Wiley etc. Her current research interests include information security, user authentication, security of wireless sensor networks, and applied mathematics.

Mohammad Reza Aref received the B.Sc. degree in 1975 from the University of Tehran, Iran, and the M.Sc. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. He was a Faculty member of Isfahan University of Technology from 1982 to 1995. He has been a Professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 230 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.

Appendix: The HLPSL Specification

At first, the initiator HAN_{GW_i} receives the start signal and then generates random number a and current timestamp t_i, computes $A = g^a, TID_i = ID_i \oplus H(P_j^a)$ and $V = a + s_i H(ID_i \| A \| t_i) \pmod p$, and finally sends the message $\langle t_i, A, TID_i, V \rangle$ to BAN_{GW_j} via open channel. By the declarations secret({IDi, IDj}, sp1, {HANgwi, BANgwj}), it means that the information $\{ID_i, ID_j\}$ are kept secret to HAN_{GW_i} and BAN_{GW_j}, whereas the declaration secret(Si, sp2, {HANgwi}) means the private key s_i of HAN_{GW_i} is kept secret to HAN_{GW_i} only, and the declaration secret(Sj, sp3, {BANgwj}) tells that the private key s_j of BAN_{GW_j} is kept secret to BAN_{GW_j} only. After receiving the message $\langle t_i, A, TID_i, V \rangle$ from HAN_{GW_i}, BAN_{GW_j} generates random number b and current timestamp t_j, computes B, L and C_j, and then sends the message $\langle t_j, B, C_j \rangle$ to HAN_{GW_i} through public channel. After receiving this message, HAN_{GW_i} sends another message $\langle t_m, C \rangle$ to BAN_{GW_j} by generating current timestamp t_m and demand reuest message M_i encrypted with the generated session key $K_{ij} = H(ID_i \| ID_j \| A \| B \| B^a)$.

The declaration witness (HANgwi, BANgwj, han_ban_a, A') means that HAN_{GW_i} has freshly generated the random number a for BAN_{GW_j}, whereas witness (HANgwi, BANgwj, han_ban_ti, Ti') indicates that HAN_{GW_i} has freshly generated the current timestamp t_i for BAN_{GW_j}. Similarily, other declarations of witness are provided in the roles of HAN_{GW_i} (Figure 4) and BAN_{GW_j} (Figure 5). The declaration request(BANgwj, HANgwi, ban_han_b, B') and request(BANgwj, HANgwi, ban_han_tj, Tj') mean that HAN_{GW_i}'s acceptance of b and t_j generated for HAN_{GW_i} by BAN_{GW_j}. The HLPSL specification for the role of BAN_{GW_j} is also implemented in a similar way in Figure 5.

Figure 6 shows the definitions for necessary roles - session, goal and environment. In the session segment, all the basic roles: han_gwi and ban_gwj are instanced with concrete arguments. The top-level role (environment) specifies in the specification of HLPSL, which contains the global constants and a composition of one or more sessions, where the intruder (i) plays some roles as legitimate users. The intruder also participates in the execution of protocol as a concrete session. The current version of HLPSL supports the standard authentication and secrecy goals. In the implementation, the following three secrecy goals and five authentications are checked:

- secrecy_of sp1: It represents that $\{ID_i, ID_j\}$ are kept secret to HAN_{GW_i} and BAN_{GW_j}.
- secrecy_of sp2: It represents that the private key s_i of HAN_{GW_i} is kept secret to HAN_{GW_i} only.
- secrecy_of sp3: It represents that the private key s_j of BAN_{GW_j} is kept secret to BAN_{GW_j} only.
- authentication_on han_ban_a: HAN_{GW_i} generates a random number a, where a is only known to HAN_{GW_i}. If the BAN_{GW_j} gets a from the message $\langle t_i, A, TID_i, V \rangle$, it authenticates HAN_{GW_i} based on a.
- authentication_on han_ban_ti: HAN_{GW_i} generates current timestamp t_i. If the BAN_{GW_j} receives t_i from the message $\langle t_i, A, TID_i, V \rangle$, it authenticates HAN_{GW_i} based on t_i.
- authentication_on ban_han_b: BAN_{GW_j} generates a random number b, where b is only known to BAN_{GW_j}. If the HAN_{GW_i} receives b from the message $\langle t_j, B, C_j \rangle$, it authenticates BAN_{GW_j} based on b.
- authentication_on ban_han_tj: BAN_{GW_j} generates current timestamp t_j. If the HAN_{GW_i} receives t_j from the message $\langle t_j, B, C_j \rangle$, it also authenticates BAN_{GW_j} based on t_j.
- authentication_on han_ban_tm: HAN_{GW_i} generates current timestamp t_m. If the BAN_{GW_j} receives t_m from the message $\langle t_m, C_j \rangle$, it authenticates HAN_{GW_i} based on t_m.

The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 186)
http://www.isecure-journal.org

Persian Abstract

یک طرح تبادل کلید سبک وزن حافظ حریم خصوصی برای شبکه هوشمند انرژی

مجید بیات[۱]، زهرا زارع جوشقانی[۲]، آشوک کومار داس[۳]، پیتام سینگ[۴]، سارو کوماری[۵]، محمدرضا عارف[۲]

[۱]دانشکده کامپیوتر، دانشگاه شاهد، تهران، ایران
[۲]دانشکده برق، دانشگاه صنعتی شریف، تهران، ایران
[۳]مرکز امنیت موسسه فناوری اطلاعات، حیدرآباد، هند
[۴]دانشکده ریاضی، موسسه ملی فناوری موتیلال نهرو، الله آباد، هند
[۵]دانشکده ریاضی، دانشگاه چ چاران سینگ، میروت، اوتار پرادش، هند

مفهوم شبکه هوشمند برای اصلاح شبکه برق با استفاده از فن‌آوری جدید اطلاعات و ارتباطات معرفی شده است . شبکه هوشمند به اطلاعات برخط مصرف برق برای نظارت بر مصرف و ارائه خدمات مورد نیاز، نیاز دارد و برای این مسئله ، ارتباطات دو جهته اطلاعات ضروری است. امنیت و حریم خصوصی الزامات مهمی است که باید در ارتباطات برقرار شود. به دلیل طراحی پیچیده سیستم‌های شبکه هوشمند و استفاده متفاوت از فن‌آوری‌های جدید، فرصتهای بسیاری برای مهاجمان برای حمله ایجاد کرده است که می‌تواند مشکلات مهمی برای مشتریان به وجود آورد. طرح‌های احراز هویت حافظ حریم خصوصی یک عنصر مهم برای توسعه امن شبکه هوشمند انرژی است. اخیراً، محمود و همکاران [۱] یک طرح احراز هویت سبک وزن برای ارتباطات شبکه هوشمند ارایه داده‌اند و ادعا می‌کند که آن طرح الزامات امنیتی شبکه‌های هوشمند انرژی را برآورده می‌کند. متأسفانه متوجه شدیم که طرح آن‌ها دارای برخی از آسیب‌های امنیتی است و ویژگی‌های امنیتی لازم برای استفاده در شبکه هوشمند انرژی را ندارد. برای برطرف کردن این اشکالات، ما یک طرح احراز هویت حافظ حریم خصوصی سبک وزن، کارآمد و ایمن برای شبکه هوشمند انرژی ارایه می‌کنیم. امنیت طرح پیشنهادی را بطور فرمال با BAN و AVISPA بررسی خواهیم کرد. بررسی‌های امنیتی و کارایی طرح پیشنهادی و مقایسه با طرح‌های مرتبط کارایی و امنیت طرح ما را مورد تاکید قرار می‌دهد.

واژه‌های کلیدی: شبکه هوشمند انرژی، احراز اصالت، حریم خصوصی، BAN، AVISPA.