5-12-2019

Anonymous and Efficient Message Authentication Scheme for Smart Grid

Libing Wu
Wuhan University, China

Jing Wang
Wuhan University, China

Sherali Zeadally
University of Kentucky, szeadally@uky.edu

Debiao He
Guilin University of Electronic Technology, China

Anonymous and Efficient Message Authentication Scheme for Smart Grid

Notes/Citation Information
Published in *Security and Communication Networks*, v. 2019, article ID 4836016, p. 1-12.

Digital Object Identifier (DOI)
https://doi.org/10.1155/2019/4836016

Hindawi
Security and Communication Networks
Volume 2019, Article ID 4836016, 12 pages
https://doi.org/10.1155/2019/4836016

Research Article

Anonymous and Efficient Message Authentication Scheme for Smart Grid

Libing Wu,[1,2] Jing Wang,[1,2] Sherali Zeadally,[3] and Debiao He [2,4]

[1]*School of Computer Science, Wuhan University, Wuhan, China*
[2]*Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, China*
[3]*College of Communication and Information, University of Kentucky, USA*
[4]*School of Cyber Science and Engineering, Wuhan University, Wuhan, China*

Correspondence should be addressed to Debiao He; hedebiao@163.com

Received 12 December 2018; Revised 10 April 2019; Accepted 22 April 2019; Published 12 May 2019

Academic Editor: Roberto Di Pietro

Smart grid has emerged as the next-generation electricity grid with power flow optimization and high power quality. Smart grid technologies have attracted the attention of industry and academia in the last few years. However, the tradeoff between security and efficiency remains a challenge in the practical deployment of the smart grid. Most recently, Li et al. proposed a lightweight message authentication scheme with user anonymity and claimed that their scheme is provably secure. But we found that their scheme fails to achieve mutual authentication and mitigate some typical attacks (e.g., impersonation attack, denial of service attack) in the smart grid environment. To address these drawbacks, we present a new message authentication scheme with reasonable efficiency. Security and performance analysis results show that the proposed scheme can satisfy the security and lightweight requirements of practical implementations and deployments of the smart grid.

1. Introduction

The explosive growth in mobile data services has paved the way for wireless communications to be achieved with lower energy consumption, higher throughout, and better quality of service [1]. The smart grid is one of the most significant technologies for developing smart homes and, as a result, we have witnessed an increase in interest among researchers and engineers in these technologies. Besides the one-way information flow communication as in the traditional power grid, the smart grid incorporates two-way communications to provide reliability, efficiency, and security for the electric system, where there are many machines (i.e., smart meters, sensing devices, control systems, and other household applications) involved to enable these two-way communications [2, 3].

Generally, network communication forms the core of the electric system automation applications of the smart grid. The deployment of one-way information flow communication networks is similar to that in the traditional smart grid. As for the two-way information flow communication network, it involves a neighborhood gateway which collects the electricity consumption records from corresponding consumers via wireless network connections [4]. Next, the neighborhood gateway sends its collected data to the control center for detailed consumption analysis via a wired network connection. Finally, the control center responds with real-time pricing information to the smart grid consumers or sends the electric control information to relieve the burden of electricity demand peak. At the consumer's side, the device communicating with the neighborhood gateway is the smart meter which is resource-constrained and is responsible for collecting the electricity consumption reports through its connection with various household appliances. Figure 1 depicts the communication architecture for smart grid (and the entities concluded in a home area network (HAN) are some household appliances).

To enable network communications in the above architecture, it is desirable to choose the Internet Protocol-based communication technologies for the smart grid. Inevitably, such networks are prone to a number of external attacks, such as impersonation attack, tracking attack, and denied

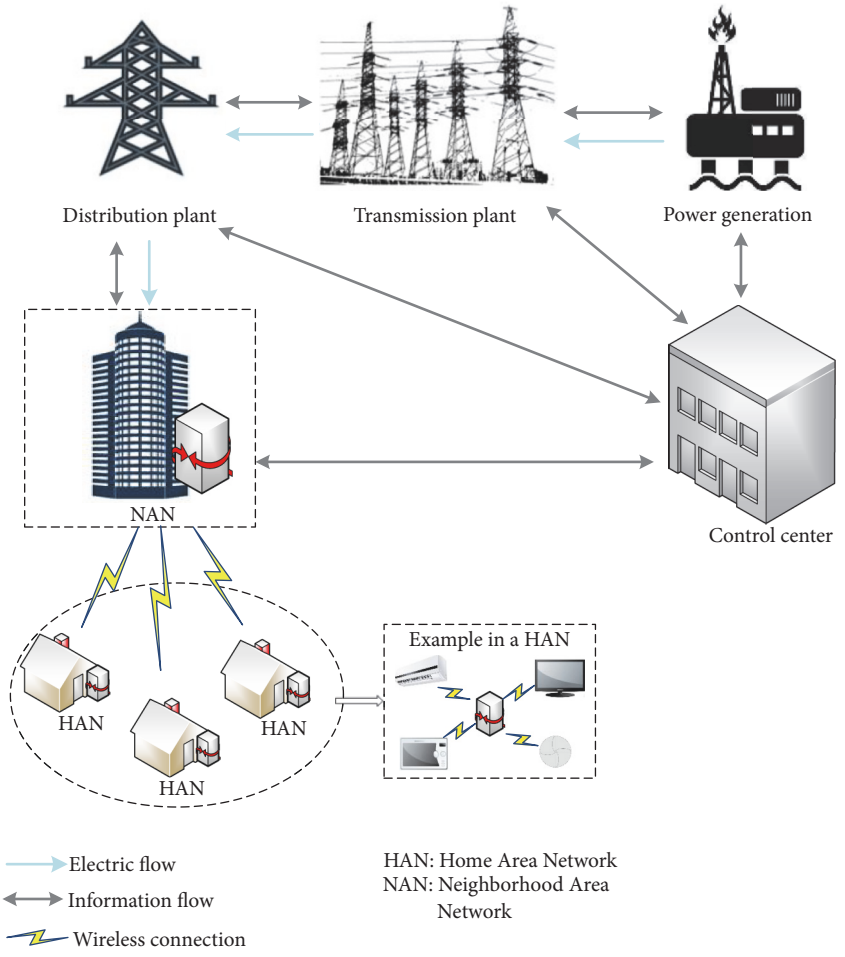


Figure 1: Simplified communication architecture of smart grid (updated from [4]).

of service (DoS) attack [6]. Additionally, a large volume of sensitive data that directly impact user privacy is transmitted over these networks. Consequently, it is crucial to ensure that unauthorized entities cannot access such transmitted information or communicate with the information technologies elements in the smart grid communication systems.

Authentication and key agreement protocols are key technologies that can ensure the security of an information system. Together, they ensure the legitimacy and authenticity of a user's identity and provide an agreed session key for secure communication between entities in a network. According to recent researches [7–10], several authentication schemes for smart grid were proposed over the last several years. We identify two major limitations of many of these recently proposed authentications for smart grid:

(i) *The computation cost of these schemes is not practical for smart grid environment:*

in a smart grid, most of smart things and applications connected to the Internet are constrained to computation capabilities. However, the smart devices (e.g., smart meters) in these authentication schemes are expected to perform some compute-intensive operations, such as the map-to-point hash and bilinear pairing operations.

(ii) *Important security properties or functions are not provided by these schemes:*

these schemes have various vulnerabilities that can be exploited in different types of attacks to the smart grid networks, such as the impersonation attack and denial of service attack. Some of these schemes cannot provide secure mutual authentication, key agreement, and user anonymity. These limitations seriously hinder their practical deployment and implementation in the smart grid environment.

Most recently, Li et al. [5] proposed an anonymous and lightweight message authentication scheme for smart grids. They only used some very lightweight cryptographic operations in their scheme, e.g., bitwise XOR operation and one-way hash functions. They also claimed that their scheme is provably secure and provides many necessary functions and security properties. However, we demonstrate that their scheme cannot provide secure mutual authentication and

resistance against DoS attacks, which can seriously affect the availability of network communication systems. Since the message transmitted over the grid communication networks is delay-sensitive, these networks of smart grids are much more focused on the message delay than the data throughout when compared with the general Internet. Thus, Li et al.'s scheme is not practical in the deployment of smart grids. To address these weaknesses, we then propose an improved scheme and show that it is provably secure in Section 6.

The remainder of this paper is organized as follows. In the next two sections, we briefly review related works and relevant preliminaries, respectively. In Section 4, we review Li et al.'s scheme and identify the design weaknesses of their scheme. In Section 5, we describe our improved message authentication scheme for the smart grid. In Sections 6 and 7, we analyze the security and evaluate the performance of our proposed scheme respectively. Finally, we make some concluding remarks in the last section.

2. Related Work

In the last decade, several cryptographic protocols including digital signature [11], encryption [12, 13], data aggregation [14, 15], secure data storage [16–18], and authentication schemes [9, 19] have been proposed as solutions to secure the smart grid by academia and industry [20]. The authentication scheme is the first line of defense to protect data security and enforce privacy protection for smart grids, and it is an important requirement in the deployment of smart grids.

Tsai and Lo [8] proposed an anonymous key distribution scheme to provide secure communications for smart grids by integrating identity-based signature and identity-based encryption. In their scheme, it is fairly easy for smart meters to authenticate each other, while some bilinear pairing operations are introduced. Later, Odelu et al. [21] pointed out that Tsai and Lo's scheme fails to support SK-security and credential privacy of smart meters and then proposed a new authentication key agreement scheme for the smart grid environment to solve the vulnerabilities in [8].

Chim et al. proposed a gateway-assisted authentication for power usage information with privacy preservation for smart grids, which allowed the smart meters to aggregate power usage information [22]. Chan and Zhou proposed a two-factor cyberphysical device authentication scheme to resist coordinated cyberphysical attacks in a smart grid (SG) environment by combining a novel contextual factor and conventional authentication factor [23]. Then, Wazid et al. proposed a secure three-factor authentication scheme for renewable-energy-based smart grid environment, which can provide password and biometric update and smart meter anonymity [19]. Li et al. [24] also proposed a three-factor authentication scheme for smart grid and solved the shortcomings (i.e., wrong password detection mechanism, vulnerability in DoS attacks) in [25].

Li et al. claimed that many of the existing authentication schemes for wireless sensor networks more or less suffer from various weaknesses, so that they proposed a new secure authentication scheme with privacy preservation based on elliptic curve cryptography (ECC) for industrial Internet of things [26]. Mahmood et al. also proposed an ECC-based privacy-preserving authentication for smart grid communications with high efficiency by reducing some complex cryptographic operations [27]. Koo et al. also investigated both security and privacy into smart grid systems; they proposed a provably secure scheme with privacy-preserving aggregation and multisource smart meters authentication [28]. Before this, He et al. had proposed two related data aggregation schemes that are resistant against insider attacks in smart grid systems [14, 29].

Shen et al. designed two lightweight authentication protocols and a group key establishment algorithm between sensor nodes and personal digital assistants for wireless body area networks [30, 31]. Their proposed protocols were aimed at resource-constrained devices and therefore they can be applied to smart grid systems. Ennahbaoui and Idrissi [32] designed a zero-knowledge authentication and intrusion detection system for secure smart grids. In [33], Aujla et al. argued that traditional TCP/IP-based networks are not suitable for most smart applications, so they proposed an SDN-enabled multiattribute secure communication model for smart grids. Most recently, Li et al. [5] proposed a provably secure message authentication scheme with high efficiency for smart grids. However, in this work, we will demonstrate the scheme fails to provide mutual authentication and cannot mitigate the impersonation attacks and DoS attacks.

2.1. Our Contributions. In this subsection, we summarize the main contributions of this work as follows:

(i) First, we propose a new anonymous message authentication scheme for smart grid. The proposed scheme addresses the weaknesses in Li et al.'s scheme with desire efficiency.

(ii) Second, we make an in-depth security analysis to demonstrate out proposed scheme is provably secure and can fulfill those security requirements of the smart grid environment.

(iii) Finally, we evaluate the performance of our proposed scheme and compare it with that in Li et al.'s scheme. The comparison results show that our scheme is more suitable for the practical deployment of the smart grid.

3. Preliminaries

Next, we present the threat models, some notations, and two mathematical problems used in this paper.

3.1. Notations. We use the following notations in this paper:

(i) HAN_{GW_i}: the i-th smart meter gateway of the home area network (HAN).

(ii) NAN_{GW_j}: the j-th smart meter gateway of the neighborhood area network (NAN).

(iii) $\mathbb{G}$: a cyclic multiplication group.

(iv) q: a strong prime integer as the order of $\mathbb{G}$.

(v) g: the generator of $\mathbb{G}$.

(vi) h: the secure hash function, where $h : \{0,1\}^* \longrightarrow Z_q$.

(vii) h': the secure hash function, where $h' : \{0,1\}^* \longrightarrow \{0,1\}^{\log_2 q + |ID|}$.

(viii) ID_i: the real identity of HAN_{GW_i}, where $ID_i \in \{0,1\}^*$.

(ix) ID_j: the real identity of NAN_{GW_j}, where $ID_j \in \{0,1\}^*$.

(x) $\oplus$: the exclusive-OR operation.

(xi) Δt: the uplimited time interval.

(xii) $Pr[E]$: the probability of event E.

3.2. Mathematical Problems. Let $\mathbb{G}$ be a cyclic multiplication group with generator g and a strong prime integer q as its order, so that $p = 2 \times q + 1$ is also a large prime integer. For any number $a \in Z_q^*$, g^a mod p is included in $\mathbb{G}$. For clarity, we omit the expression "mod p" in this paper. The following two mathematical problems are the security foundation of the proposed scheme in Section 5.

(1) *Discrete Logarithm (DL) Problem.* Given two elements $(g, g^a) \in \mathbb{G}$, the goal is to compute the value of $a \in Z_q^*$, which is hard for a polynomial function with in polynomial time.

(2) *Computational Diffie-Hellman (CDH) Problem.* Given three elements $(g, g^a, g^b) \in \mathbb{G}$, where $a, b \in Z_q^*$ are kept secret, the goal is to compute the value of $g^{ab} \in \mathbb{G}$, which is hard for a polynomial function within polynomial time.

3.3. Network Model. In our network model, we focus on the communication security between the neighborhood gateway and the smart meter. As shown in Figure 2, we assume that a neighborhood area network (NAN) covers a number of home area networks (HANs, e.g., HAN_1, HAN_2, HAN_3), where the smart meter is a communication center. We also assume the smart meter as a gateway in the HAN.

(i) Registration center (RC): the RC represents a trusted third party that is responsible for generating all system parameter, and secret values (i.e., private key) for each communication party in the system.

(ii) Neighborhood gateway (NAN-GW): the NAN-GW represents a gateway deployed in the NAN. It is in charge of receiving the consumption reports from each HAN-GW and then sends them to the control center. The main function of the NAN-GW is to detect the replay attack, impersonation attack, and other malicious attacks.

(iii) Home gateway (HAN-GW): the HAN-GW represents a gateway deployed in the HAH. It is equipped with a smart meter in order to collect the consumption reports and then transmits them to the NAN-GW. The HAN-GW is resource-constrained and vulnerable to many network attacks.

4. Cryptanalysis of Li et al.'s Scheme

In this section, we briefly review the provably secure message authentication scheme proposed by Li et al. For more details, readers can refer to [5]. Focusing on the authentication phase, we demonstrate that this phase is vulnerable to the impersonation attack and the DoS attack.

4.1. Review of Li et al.'s Scheme. Li et al.'s scheme consists of three phases (i.e., initialization phase, authentication phase, and message transmission phase) and two communication parties (i.e., HAN_{GW_i} and NAN_{GW_j}). Since the initialization phase and message transmission phase are the same as described in Sections 5.1 and 5.3, we omit them in this subsection. We only present the authentication phase as depicted in Figure 3.

Step A1. HAN_{GW_i} randomly selects a number $a \in Z_q^*$ and extracts the current timestamp t_i to compute $C_1 = g^a$, $C_2 = P_j^s \oplus ID_i$ and $C_3 = a(x_i + h(ID_i \| t_i))^{-1}$.

Step A2. HAN_{GW_i} sends $M_1 = \{C_1, C_2, C_3, t_i\}$ to NAN_{GW_j}.

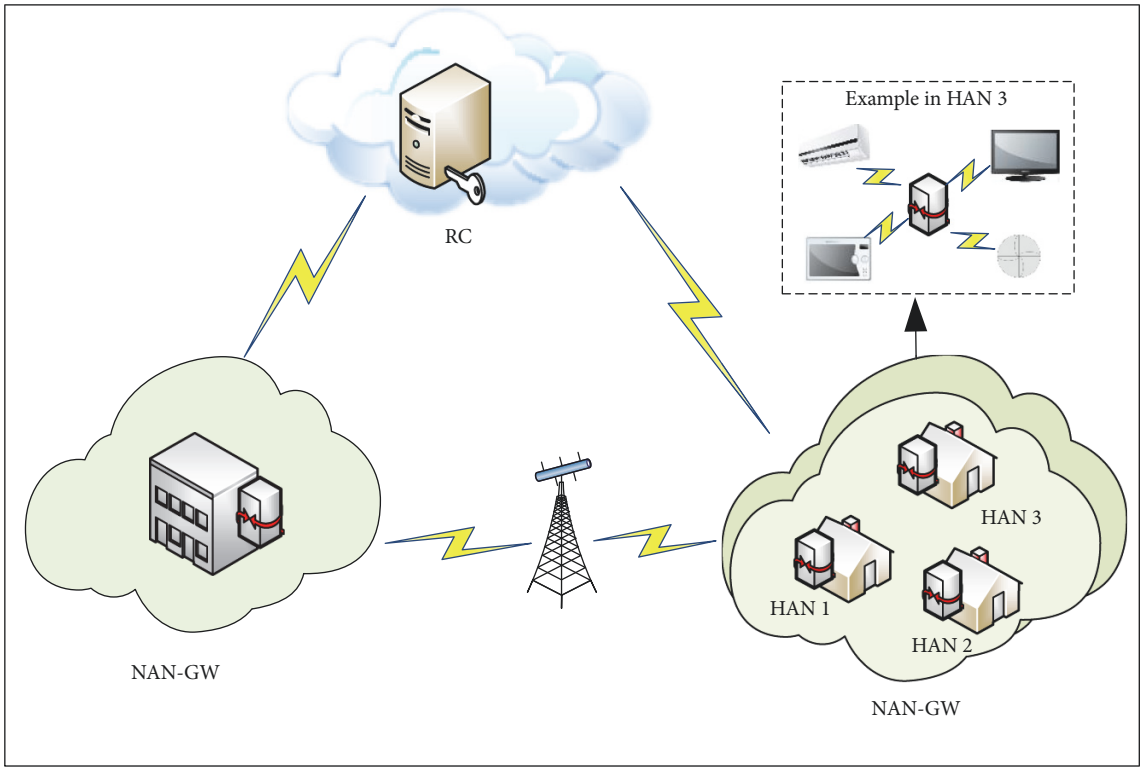
Step A3. Upon receiving message M_1, NAN_{GW_j} extracts the current timestamp t_i', checking whether $|t_i' - t_i| \le \Delta t$ holds. If so, it continues to compute $ID_i = C_2 \oplus C_1^{y_j}$ for verifying $P_i g^{h(ID_i \| t_i)})^{C_3} \stackrel{?}{=} C_1$. If the equation does not hold, it aborts the current authentication. Otherwise, it does the next step.

Step A4. NAN_{GW_j} randomly selects a number $b \in Z_q^*$ and extracts the current timestamp t_j to compute $C_4 = g^b$, $C_5 = h(C_1^{y_j} \| ID_i \| t_i) \oplus ID_j$, $sk_{N-H} = h(C_1 \| C_4 \| C_1^b \| ID_i \| ID_j)$ and $C_6 = h(ID_i \| t_i \| ID_j \| t_j \| C_1 \| C_4 \| sk_{N-H})$.

Step A5. NAN_{GW_j} sends $M_2 = \{C_4, C_5, C_6, t_i\}$ to HAN_{GW_i}.

Step A6. Upon receiving message M_2, HAN_{GW_j} extracts the current timestamp t_j', checking whether $|t_j' - t_j| \le \Delta t$ holds. If it holds, it computes $ID_j = C_5 \oplus h(P_j^a \| ID_i \| t_j)$, $sk_{H-N} = h(C_1 \| C_4 \| C_4^a \| ID_i \| ID_j)$. Then, it checks the correctness of $C_6 = h(ID_i \| t_i \| ID_j \| t_j \| C_1 \| C_4 \| sk_{H-N})$ to determine whether aborts this communication.

4.2. Design Weaknesses in Li et al.'s Scheme. With superior performance and desired properties over the related works, Li et al.'s scheme seems quite promising from the perspective of desirable features which their scheme supports. However, its potential threats in some realistic attack scenarios go beyond the provable security model, the security analysis of their scheme is insufficient. We will show that their scheme fails to achieve mutual authentication by verifying $(P_i g^{h(ID_i \| t_i)})^{C_3} = C_1$ at the NAN_{GW_j}'s side. Additionally, their scheme cannot resist impersonation attack where an attacker $\mathcal{A}$ forges a message M_1 to impersonate HAN_{GW_i}.



RC: Registration Center

NAN-GW: the Gateway in Neighborhood Area Network

HAN: Home Area Network

Figure 2: A simplified communication network model (updated from [1]).

HAN_{GW_i} $(x_i, P_i = g^{x_i})$		NAN_{GW_j} $(x_j, P_j = g^{x_j})$
Randomly chooses $a \in Z_q^*$		
Computes $C_1 = g^a$		
$C_2 = P_j^a \oplus ID_i$		
$C_3 = a(x_i + h(ID_i \Vert t_i))^{-1}$		
	$M_1 = \{C_1, C_2, C_3, t_i\}$ ⟶	
		Gets t_i'
		Checks $\vert t_i' - t_i \vert \le \Delta T$
		Computes $ID_i = C_2 \oplus C_1^{x_j}$
		Checks $(P_i g^{h(ID_i \Vert t_i)})^{C_3} = C_1$
		Randomly chooses $b \in Z_q^*$
		Computes $C_4 = g^b$
		$C_5 = h(C_1^{x_j} \Vert ID_i \Vert t_j) \oplus ID_j$
		$sk_{N-H} = h(C_1 \Vert C_4 \Vert C_1^b \Vert ID_i' \Vert ID_j)$
		$C_6 = h(ID_i \Vert t_i \Vert ID_j \Vert t_j \Vert C_1 \Vert C_4 \Vert sk_{N-H})$
	⟵ $M_2 = \{C_4, C_5, C_6, t_j\}$	
Gets t_j'		
Checks $\vert t_j' - t_j \vert \le \Delta T$		
Computes $ID_j = h(P_j^a \Vert ID_i \Vert t_j) \oplus C_5$		
$sk_{H-N} = h(C_1 \Vert C_4 \Vert C_4^a \Vert ID_i \Vert ID_j)$		
Verifies $C_6 = h(ID_i \Vert t_i \Vert ID_j \Vert t_j \Vert C_1 \Vert C_4 \Vert sk_{H-N})$		

Figure 3: Authentication phase of Li et al.'s scheme.

Next we investigate the following new but realistic attacking scenario. Suppose the identity ID_i is somehow known to an attacker $\mathscr{A}$ as in the case when $\mathscr{A}$ is familiar to the user and guesses the ID_i via the user's personal information. Since the authentication message $M_1 = \{C_1, C_2, C_3, t_i\}$ is transmitted over an open channel, it is easy for $\mathscr{A}$ to intercept M_1 during any authentication process. Suppose $\mathscr{A}$ has obtained two messages $M_1^1 = \{C_1^1, C_2^1, C_3^1, t_i^1\}$ and $M_1^2 = \{C_1^2, C_2^2, C_3^2, t_i^2\}$, where $C_1^1 = g^{a_1}$, $C_1^2 = g^{a_2}$ and a_1, a_2 are unknown to the attacker. $\mathscr{A}$ can impersonate HAN_{GW_i} by forging any request message $M_1^* = \{C_1^*, C_2^*, C_3^*, t_i^*\}$ with real-time t_i^* as shown by following steps.

Step 1. Compute $h_1 = h(ID_i \parallel t_i^1)$, $h_2 = h(ID_i \parallel t_i^2)$, $h^* = h(ID_i \parallel t_i^*)$, and $P_1 = C_2^1 \oplus ID_i$, $P_2 = C_2^2 \oplus ID_i$.

Step 2. Select two variables σ_1, σ_2 to construct equations

$$\begin{aligned} C_3^* &= \sigma_1 \cdot C_3^1 + \sigma_2 \cdot C_3^2 \\ h^* \cdot C_3^* &= \sigma_1 \cdot h_1 \cdot C_3^1 + \sigma_2 \cdot h_2 \cdot C_3^2 \end{aligned} \tag{1}$$

Step 3. Compute one of solutions to above equations, such as

$$\begin{aligned} \sigma_1 &= 1 \\ \sigma_2 &= \frac{(h^* - h_1)\, C_3^1}{(h_2 - h^*)\, C_3^2} \end{aligned} \tag{2}$$

Step 4. Compute $C_1^* = (C_1^1)^{\sigma_1} \cdot (C_1^2)^{\sigma_2}$, $C_2^* = ((P_1)^{\sigma_1} \cdot (P_2)^{\sigma_2}) \oplus ID_i$, and $C_3^* = \sigma_1 \cdot C_3^1 + \sigma_2 \cdot C_3^2$.

Step 5. Send $M_1^* = \{C_1^*, C_2^*, C_3^*, t_i^*\}$ to a valid NAN_{GW_j}.

Correctness. Upon receiving the message M_1^* from $\mathscr{A}$, NAN_{GW_j} first checks the freshness of t_i^*. Then, it computes $ID_i^* = C_2^* \oplus (C_1^*)^{y_j}$. Since

$$\begin{aligned} C_2^* &= \left((P_1)^{\sigma_1} \cdot (P_2)^{\sigma_2}\right) \oplus ID_i \\ &= \left(\left(P_j^{a_1}\right)^{\sigma_1} \cdot \left(P_j^{a_2}\right)^{\sigma_2}\right) \oplus ID_i \\ &= \left(\left(g^{a_1\sigma_1}\right)^{y_j} \cdot \left(g^{a_2\sigma_2}\right)^{y_j}\right) \oplus ID_i \\ &= \left(\left(C_1^1\right)^{\sigma_1} \cdot \left(C_1^2\right)^{\sigma_2}\right)^{y_j} \oplus ID_i = \left(C_1^*\right)^{y_j} \oplus ID_i \end{aligned} \tag{3}$$

we obtain $ID_i^* = C_2^* \oplus (C_1^*)^{y_j} = ID_i$. Next, NAN_{GW_j} checks whether $(P_i g^{h(ID_i \| t_i^*)})^{C_3^*} \stackrel{?}{=} C_1^*$. According to Step 2 above, we can get

$$\begin{aligned} \left(P_i g^{h(ID_i \| t_i^*)}\right)^{C_3^*} &= P_i^{C_3^*} \cdot g^{h^* C_3^*} \\ &= P_i^{\sigma_1 C_3^1 + \sigma_2 C_3^2} \cdot g^{\sigma_1 h_1 C_3^1 + \sigma_2 h_2 C_3^2} \\ &= \left(P_i^{C_3^1} \cdot g^{h_1 C_3^1}\right)^{\sigma_1} \cdot \left(P_i^{C_3^2} \cdot g^{h_1 C_3^2}\right)^{\sigma_2} \\ &= \left(C_1^1\right)^{\sigma_1} \cdot \left(C_1^2\right)^{\sigma_2} = C_1^* \end{aligned} \tag{4}$$

Therefore, an attacker $\mathscr{A}$ can pass NAN_{GW_j}'s authentication without knowing a HAN_{GW_i}'s private key. As a result, $\mathscr{A}$ manages to make NAN_{GW_j} believe that he/she is a valid HAN_{GW_i} and continuously execute authentication operations. Thus, an external attacker can break the security of mutual authentication and launch the DoS attack on the smart grid by impersonating a legal HAN_{GW_i} gateway to connect with the corresponding NAN_{GW_j}. As a consequence, the smart grid network system cannot reject the connection of a malicious IP address by detecting the invalid data packages received, and thus it is susceptible to DoS attacks, which will lead to an increase in message delay.

Effectiveness. It is worth noting that the above attack is very effective because it only requires a passive eavesdropping attacker and involves a few lightweight cryptographic operations, such as addition, multiplication, exponentiation, and hash operations. For example, to get a solution in Step 3 and forge a successful authentication message M_1, we only require three general hash operations, six multiplication operations, one division operation, four exponentiation operations, and three addition/subtraction operations. Given the running time of each operation referred in Li et al.'s scheme [5], the total time for $\mathscr{A}$ to successfully implement an attack is about 1.396ms.

5. The Proposed Scheme

To overcome the weakness of Li et al.'s scheme, we propose an improved anonymous message authentication scheme for the smart grid. Similar to Li et al.'s scheme, our protocol also has three phases: the initialization phase, the authentication and key agreement phase, and the message transmission phase.

5.1. Initialization Phase. In this phase, the registration center (RC) generates the system parameters and private-public key pair for each registered entity (i.e., HAN_{GW_i} and NAN_{GW_j}) as follows.

Step I1. The RC chooses a multiplication cyclic group $\mathbb{G}$ with order q, and the generator is g. Next, the RC selects a secure one-way hash function $h'(\cdot) : \{0,1\}^* \longrightarrow \{0,1\}^{\log_2 q + |ID|}$ and a secure hash function $h(\cdot) : \{0,1\}^* \longrightarrow Z_q^*$.

Step I2. For each registered entity, RC generates a distinct random number x as private key and computes g^x as the corresponding public key. Here, let $x_i \in Z_q^*$ be the i-th HAN-GW's private key, and $P_i = g^{x_i}$ be i-th HAN-GW's public key.

Step I3. The RC sends the key pair (x_i, P_i) to HAN_{GW_i} (i.e., the i-th HAN-GW) via a secure channel, where P_i can be revealed to others.

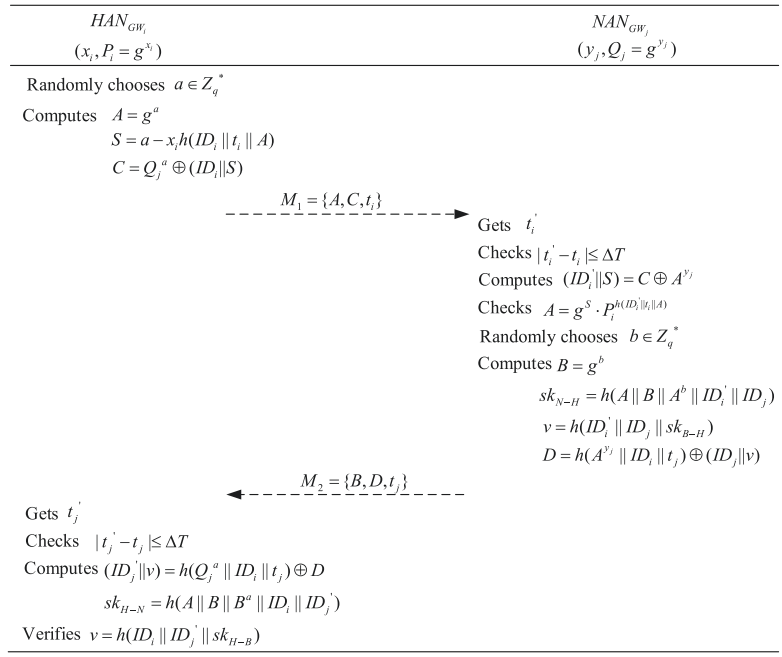


Figure 4: Authentication phase of the proposed scheme.

Similarly, the j-th NAN-GW can obtain its own key pair as $(y_j, Q_j = g^{y_j})$ from the RC as described in *Step I3*.

5.2. Authentication Phase. In this phase, HAN_{GW_i} and NAN_{GW_j} authenticate with each other. In addition, a temporary session key is created and used for encrypting subsequent transmitted messages. As depicted in Figure 4, the details are described as follows.

Step A1. HAN_{GW_i} first chooses a random number a from group Z_q^* and assigns up the current timestamp t_i. Then, HAN_{GW_i} computes $A = g^a, C = Q_j^a \oplus (ID_i \parallel S)$ and $S = a - x_i h(ID_i \parallel t_i \parallel A)$.

Step A2. HAN_{GW_i} sends the plain message $M_1 = (A, C, t_i)$ to NAN_{GW_j} via a public channel.

Step A3. Upon receiving message M_1 at time t_i', NAN_{GW_j} first checks the freshness of the timestamp t_i by equation $|t_i' - t_i| \leq \Delta t$. If it holds, NAN_{GW_j} computes $ID_i' = C \oplus A^{y_j}$ and further verifies the correctness of $A \stackrel{?}{=} g^S \cdot P_i^{h(ID' \| t_i \| A)}$. If the final equation does not hold, NAN_{GW_j} aborts the authentication process. Otherwise, it continues to the next step.

Step A4. NAN_{GW_j} selects a random number b from group Z_q^* and gets the current timestamp t_j. Similarly, HAN_{GW_i} computes $B = g^b$ and the temporary session key $sk_{N-H} = h(A \parallel B \parallel A^b \parallel ID_i' \parallel ID_j$. Finally, HAN_{GW_i} computes $v = h(ID_i' \parallel ID_j, sk_{N-H}), D = h'(A^{y_j} \parallel ID_i' \parallel t_j) \oplus (ID_j \parallel v)$.

Here, we assume that HAN_{GW_i} already knows the identity of NAN_{GW_j} (i.e., ID_j) because it is a control smart meter among several HAN_{GW_i} in a specific neighborhood.

Step A5. NAN_{GW_j} sends the plain message $M_2 = (B, D, t_j)$ to HAN_{GW_i} via a public channel.

Step A6. Upon receiving message M_2, HAN_{GW_i} assigns the current timestamp t_j' and checks $|t_j' - t_j| \leq \Delta t$. If it does not hold, HAN_{GW_i} aborts this authentication. Otherwise, HAN_{GW_i} first computes $(ID_j' \parallel v') = h'(Q_j^a \parallel ID_i \parallel t_j) \oplus D, sk_{H-N} = h(A \parallel B \parallel B^a \parallel ID_i \parallel ID_j')$. Then HAN_{GW_i} verifies the correctness $v' \stackrel{?}{=} h(ID_i \parallel ID_j' \parallel sk_{H-N})$. If it holds, HAN_{GW_i} confirms that the temporary session key sk_{H-N} is associated with NAN_{GW_j}. Otherwise, HAN_{GW_i} aborts this authentication process.

5.3. Message Transmission Phase. In this phase, a secure symmetric encryption algorithm (i.e., Advanced Encryption Standard, AES) and a secure one-way hash function are used to guarantee the message's confidentiality and integrity. The details are as follows.

Step M1. HAN_{GW_i} periodically collects user's current electricity consumption report M_i and computes the value of $H_i = h(M_i \parallel T_i)$, where T_i is the current timestamp. Then, HAN_{GW_i} encrypts the message M_i as $C_i = Enc(M_i \parallel T_i \parallel H_i)$ by using the above agreed session key sk_{H-N}, and sends C_i to NAN_{GW_j} over a public channel.

Step M2. After receiving C_i at time T_i', NAN_{GW_j} runs the decryption algorithm Dec to get the corresponding plaintext of C_i with session key sk_{N-H}. The plaintext is in the form of $M_i \parallel t_i \parallel H_i$. NAN_{GW_j} further verifies $|T_i' - T_i| \leq \Delta t$ and $h(M_i \parallel T_i) \stackrel{?}{=} H_i$ to confirm the freshness and integrity of the received message.

6. Security Analysis and Comparisons

In this section, we first apply the following security model to prove that the proposed scheme is provably secure. Secondly, we make a further discussion to demonstrate that it can resist various well-known attacks along with the security requirements for smart grid.

6.1. Security Model. We assume that there are two entities HAN_{GW_i} and NAN_{GW_j} in a message authentication scheme Π. Let $HAN_{GW_i}^l$ and $NAN_{GW_j}^l$ denote the l-th instance of HAN_{GW_i} and NAN_{GW_j} respectively. If the two entities do not need to be distinguished, we denote the l-th instance of them as $\mathcal{I}^l$. All of them can have multiple instances and they are allowed to execute the scheme concurrently.

Definition 1 (adversary abilities). We use some oracles played between an adversary $\mathcal{A}$ and a simulator $\mathcal{C}$ to prove the security of the proposed scheme. $\mathcal{A}$ is able to know all the public parameters of HAN_{GW_i} and NAN_{GW_j} and control the network. Moreover, $\mathcal{A}$ can execute the following queries and get corresponding answers as follows:

(i) $h(m_t)$: $\mathcal{C}$ maintains a table L_h (or $L_{h'}$) that is initialized to empty. Upon receiving the query, $\mathcal{C}$ checks if (m_t, r_t) is recorded in L_h, if so, $\mathcal{C}$ returns r_i to $\mathcal{A}$. Otherwise, $\mathcal{C}$ chooses a random number r_i and outputs it to $\mathcal{A}$ and then records the generated entry (m_i, r_i) into L_h (or $L_{h'}$).

(ii) $Execute(HAN_{GW_i}^l, NAN_{GW_j}^l)$: this query simulates a passive attack. $\mathcal{C}$ honestly performs the authentication scheme that allows $\mathcal{A}$ to get access to the normal authentication process and outputs M_1, M_2 as the answer.

(iii) $Send(\mathcal{I}^l, m)$: $\mathcal{A}$ executes the query with message m and $\mathcal{C}$ performs the message authentication scheme according to its specification and then returns the output result to $\mathcal{A}$.

(iv) $Reveal(\mathcal{I}^l)$: if the oracle $\mathcal{I}^{\mathcal{L}}$ has turned into the *Accept* state, $\mathcal{A}$ can get the current session key of this oracle.

(v) $Corrupt(\mathcal{I}^l)$: this oracle is used in the forward secrecy model, where $\mathcal{A}$ can get the long-term secret key of $\mathcal{I}^l$ from $\mathcal{C}$'s answer.

(vi) $Test(\mathcal{I}^l)$: this oracle tests the AKA security of the session key. As the l-th session, $\mathcal{C}$ selects a bit $b \in \{0, 1\}$, if $b = 1$, outputs the real session key as the answer. Otherwise, $\mathcal{C}$ outputs a random string with the same length as the real session key.

Definition 2 (AKA-secure). Let the probability that $\mathcal{A}$ guesses the bit b involved in the *Test* query denote $\mathcal{A}$'s advantage of breaking the scheme. More precisely, we denote the advantage as $Pr[Adv_\Pi^{aka}(\mathcal{A})] = 2Pr[b = b'] - 1$. We say a scheme Π is AKA-secure if $Pr[Adv_\Pi^{aka}(\mathcal{A})]$ is negligible for any polynomial adversary $\mathcal{A}$.

Definition 3 (MA-secure). We say a message authentication scheme for smart grid Π is mutual authentication (MA) secure if the probability $Pr[Adv_\Pi^{ma}(\mathcal{A})]$ is negligible for any polynomial adversary $\mathcal{A}$.

6.2. Formal Security Proof. In this subsection, we show that our improved scheme is provably secure for smart grid. Let E_1 denote the event that $\mathcal{A}$ can break the authentication of HAN_{GW_i} -to- NAN_{GW_j} and E_2 denote the event that $\mathcal{A}$ can break the authentication of NAN_{GW_j} -to- HAN_{GW_i}. Let E_3 denote the event that $\mathcal{A}$ can break AKA security of the improved message authentication scheme. Let $Pr[E_1] = \varepsilon_1$ and $Pr[E_2] = \varepsilon_2$ be the advantage of the events that $\mathcal{A}$ can break the authentication of HAN_{GW_i} to NAN_{GW_j} and the authentication of NAN_{GW_j} to HAN_{GW_i}, respectively.

Theorem 4. *The proposed scheme for the smart grid is MA-secure if both $Pr[E_1]$ and $Pr[E_2]$ are negligible.*

Proof. Assume that the adversary has executed the above-mentioned oracles in the normal manner. In particular, we consider that $\mathcal{A}$ executes the $Send(NAN_{GW_j}^l, M_1)$-query, if the simulator succeeds to compute the value of $A = g^S \cdot P_i^{h(ID_i \| t_i \| A)}$, it implies that the message $M_1 = \{A, C, t_i\}$ is valid. If $\mathcal{A}$ can produce a valid M_1, it can produce another valid message $M_1' = \{A, C', t_i'\}$, which means it can generate a valid S'. Then, $\mathcal{C}$ can get HAN_{GW_i}'s private key $x_i = h(ID_i \parallel t_i' \parallel A)/(S - S')$ due to the following equations

$$A = g^S \cdot P_i^{h(ID_i \| t_i \| A)} \tag{5}$$

and

$$A = g^{S'} \cdot P_i^{h(ID_i \| t_i' \| A)} \tag{6}$$

Based the above two equations, we get

$$1 = \frac{g^S \cdot P_i^{h(ID_i \| t_i \| A)}}{g^{S'} \cdot P_i^{h(ID_i \| t_i' \| A)}} = g^{(S + x_i h(ID_i \| t_i \| A)) - (S' + x_i h(ID_i \| t_i' \| A))} \tag{7}$$

Thus, $\mathcal{A}$ can output $x_i = h(ID_i \parallel t_i' \parallel A)/(S - S')$ as a solution of the DL problem. It is similar to [5] that the probability of forging a correct pair (A, S) is $1/pq$. Therefore, the probability that $\mathcal{C}$ can solve the DL problem is ε_1/pq, which is contradicted with the hardness of DL problem. In other words, the probability of $Pr[E_1] = \varepsilon_1$ is negligible.

Similarly, considering the query $send(HAN_{GW_i}, M_2)$, if the message M_2 can pass the verification of $\mathcal{C}$, it implies that

$\mathscr{C}$ can get a perfect hash recording including $(Q_j^a \parallel ID_i \parallel t_j)$ in $L_{h'}$, where $Q_j = g^{y_j}$. Therefore, $\mathscr{C}$ can output $Q_j^a = g^{y_j a}$ as the instance (g, g^{y_j}, g^a) of the CDH problem with the probability of $\varepsilon_2/q_{h'}$, where q_h is the bound times of hash queries. Since the CDH is hard, the probability $Pr[E_2] = \varepsilon_2$ is negligible.

To conclude, the improved scheme is MA-secure. □

Theorem 5. *The proposed scheme for smart grid is AKA-secure if $Pr[E_3]$ is negligible.*

Proof. Assume that an adversary $\mathscr{A}$ correctly guesses the value of b involved in the *Test-query* with a nonnegligible probability ε_3. We then show that there exists a simulator $\mathscr{C}$ that can solve the CDH problem.

Let E_{sk} denote the event that $\mathscr{A}$ obtains the correct session key, and let E_{H_b}, E_{N_b} denote the events that $\mathscr{A}$ guesses b in instance HAN_{GW_i} and instance NAN_{GW_j} respectively. From the Definition 2, the probability that $\mathscr{A}$ guess the correct b is at least $1/2$, and thus we can get $Pr[E_{sk}] = \varepsilon_3/2$. Furthermore, we can get the following equations:

$$\begin{aligned}
\frac{\varepsilon_3}{2} &\le Pr\left[E_{sk}\right] \\
&= Pr\left[E_{sk} \bigwedge E_{H_b}\right] \\
&\quad + Pr\left[E_{sk} \bigwedge E_{N_b} \bigwedge E_1\right] \\
&\quad + Pr\left[E_{sk} \bigwedge E_{N_b} \bigwedge \neg E_1\right] \\
&= Pr\left[E_{sk} \bigwedge E_{H_b}\right] + Pr\left[E_1\right] \\
&\quad + Pr\left[E_{sk} \bigwedge E_{N_b} \bigwedge \neg E_1\right] \\
\frac{\varepsilon_3}{2} - Pr\left[E_1\right] &\le Pr\left[E_{sk} \bigwedge E_{H_b}\right] \\
&\quad + Pr\left[E_{sk} \bigwedge E_{N_b} \bigwedge \neg E_1\right] \\
&\le Pr\left[E_{sk} \bigwedge E_{H_b}\right] + Pr\left[E_{sk} \bigwedge E_{H_b}\right]
\end{aligned} \tag{8}$$

Thus, we get $Pr[E_{sk} \bigwedge E_{H_b}] \ge (1/2)(\varepsilon_3/2 - Pr[E_1])$.

According to Theorem 4, $Pr[E_1]$ is negligible and, therefore, $Pr[E_{sk}]$ is nonnegligible. Since $\mathscr{A}$ can break the AKA security, $\mathscr{A}$ can output g^{ab} as the solution to the CDH problem of instance (g, g^a, g^b) with nonnegligible probability, which contradicts with the hardness of CDH problem. Therefore, the proposed message authentication scheme for smart grid is AKA-secure. □

6.3. Other Discussions on Security Properties. We now demonstrate how our improved scheme achieves the mutual authentication, session key agreement, user anonymity, perfect forward secrecy, and resistance to several attacks [14, 34–37].

Mutual Authentication. From the description of our proposed scheme, NAN_{GW_j} verifies the identity of HAN_{GW_i} via checking $A = g^S \cdot P_i^{h(ID_i \| t_i \| A)}$, and HAN_{GW_i} verifies the identity of NAN_{GW_j} via checking $v = h(ID_i \parallel ID_j \parallel sk_{H-N})$. The formal security analysis has proved that nobody can impersonate one of the two parties to cheat the other one by generating a valid authenticated message M_1 (or M_2) during the authentication process. Thus, our improved scheme can support mutual authentication.

Session Key Agreement. In the authentication and key agreement phase, NAN_{GW_j} and HAN_{GW_i} can independently compute the session key $sk_{N-H} = h(A \parallel B \parallel A^b \parallel ID_i' \parallel ID_j)$ and $sk_{H-N} = h(A \parallel B \parallel B^a \parallel ID_i \parallel ID_j')$, which can be used to encrypt messages in subsequent communications. Furthermore, HAN_{GW_i} can verify the correctness of the session key by recovering v (by computing Q_j^a) and matching it with its own computed $h(ID_i \parallel ID_j \parallel sk_{H-N})$. Thus, our improved scheme can achieve session key agreement.

User Anonymity. In our improved scheme, the real identity of HAN_{GW_i} is hidden by $C = Q_j^a \oplus ID_i$, where a is a random number chosen by HAN_{GW_i} and it is unknown to others. So without knowing the value of a, the only way to reveal the identity of HAN_{GW_i} is to compute $C \oplus A^{y_j}$, where C is transmitted over the public channel while y_i is the private key known only to NAN_{GW_j}. If the adversary intends to reveal HAN_{GW_i}'s real identity, the adversary needs to get the value of Q_j^a or A^{y_j} given A, Q_j, which means he/she has to solve the CDH problem. Else, the adversary cannot get HAN_{GW_i}'s real identity. Thus, our improved scheme can provide user anonymity.

Perfect Forward Secrecy. HAN_{GW_i} and NAN_{GW_j} agree with a shared session key $sk = h(A \parallel B \parallel A^b \parallel ID_i \parallel ID_j) = h(A \parallel B \parallel B^b \parallel ID_i \parallel ID_j)$ in the final step of the authentication and key agreement phase. If an attacker intends to compute the session key of a special communication, he/she has to obtain the real identity of HAN_{GW_i} and NAN_{GW_j} and compute g^{ab} from $A = g^a$ and $B = g^b$ as well. From the above analysis, he/she needs to solve the CDH problem or it cannot derive the correct session key even though he/she obtains long-term secret key. Thus, our improved scheme can provide perfect forward secrecy.

Resistance to Several Attacks. Next, we show how the improved scheme can resist tracking attack, replay attacks, impersonation attack, man-in-the-middle attack, and DoS attack.

(i) Resistance of Tracking Attack. The messages transmitted during each session phase are different and fresh as they are randomized by two random numbers $\{a, b\}$. This means an attacker cannot link any two sessions to the same user or track a user's behaviors from some sessions. Thus, our improved scheme can mitigate the tracking attack.

Table 1: Running times of related operations (millisecond).

Operations	T_{me}	T_{inv}	T_{mm}	T_{AES}	T_h
Times	0.3308	0.0463	0.0038	0.0215	0.000033

(ii) Resistance to Replay Attack. As every authenticated message (i.e., M_1, M_2) contains timestamps, which also includes in the computation of S and AID_j, an old/intercepted authenticated messages cannot pass the verification of the other party in the current time. Thus, our improved scheme can mitigate the replay attack.

(iii) Resistance to Impersonation Attack. If an attacker intends to impersonate HAN_{GW_i}, he/she has to create a legal request message M_1 that he/she needs to compute a valid S. It means that he/she needs to know the private key x_i of HAN_{GW_i}. Similarly, impersonating NAN_{GW_j} should correctly compute the value of $h'(A^{y_j} \parallel ID_i \parallel t_j)$; otherwise, it cannot pass the verification of HAN_{GW_i}. If the attacker succeeds to impersonate NAN_{GW_j}, he/she either gets the private key y_j or solves the CDH problem with the instance $\{g, A = g^a, Q_j = g^{y_j}\}$. Thus, our improved scheme can mitigate the impersonation attack.

(iv) Resistance to Mathematical Analytical Attack. We define the attack on Li et al.'s protocol to be a mathematical analytical attack, and we now prove that our proposed protocol can resist this attack. For the sake of fairness, we assume that the identity ID_i is revealed to an attacker meaning that the attacker can get the information of ID_i and many pairs of (A, C, t_i). From the structure of $C = Q_j^a \oplus (ID_i \parallel S)$, the attacker cannot construct a system of linear equations because it has no knowledge of S. Next, we compute $S = a - x_i h(ID_i \parallel t_i \parallel A)$ rather than $S = a - x_i h(ID_i \parallel t_i)$, which further breaks the linear relations between equations. Thus, our proposed protocol can resist the mathematical analytical attack even if the attacker knows the user's identity ID_i.

(v) Resistance to Man-in-the-Middle Attack. As we analyzed before, our improved scheme can provide mutual authentication, and no attacker is able to cheat HAN_{GW_i}/NAN_{GW_j} through impersonating the other party. Thus, our improved scheme can mitigate the man-in-the-middle attack.

(vi) Resistance of DoS Attack. Assuming that an attacker intends to implement the DoS attack, he/she may flood the NAN_{GW_j} with some messages. If the message can pass the verification of NAN_{GW_j}, it will cause wastage of computation and communication resources of NAN_{GW_j} when computing and transmitting the response message, which results in increased delay for data communications in the smart grid. In our improved scheme, an illegal message can be effectively detected by NAN_{GW_j} and thus aborts the current communication thereby avoiding additional unnecessary computation and communication costs. Thus, our improved scheme can provide resistance of DoS attack to some extent.

7. Performance Evaluation and Comparisons

In this section, we evaluate the performance of our improved scheme and compare it with Li et al.'s scheme [5]. For fair comparison, we use the experimental data referred in [5] to evaluate the performance of Li et al.'s scheme and our proposed scheme.

Here, we briefly recall the experimental platform and the selected parameters used in Li et al.'s scheme. The executing platform for running related cryptographic operations is a personal computer with an Intel(R) Core TM i7-4710HQ 2.50GHz processor, 8GB memory, Win8 operating system. The related operations (e.g., modular exponentiation, bilinear pairing operation) are executed based on the MIRACL C/C++ library with Visual C++ 2010. To achieve the same security level for different schemes, Li et al. chose a multiplication cyclic group consisting of 1024-bit integers.

Let AES and 160-bit SHA1 algorithms be the symmetric encryption algorithm and hash function to handle messages in the schemes. Note that each block in AES is 128 bits. The following notations denote the average running times of related cryptographic operations and the corresponding results are presented in Table 1. Here, we ignore the XOR, modular addition operations from the comparison because their running times are negligible.

(i) T_{me}: The running time of a modular exponentiation operation.

(ii) T_{inv}: The running time of a modular inversion operation.

(iii) T_{mm}: The running time of a modular multiplication operation.

(iv) T_{AES}: The running time of a AES encryption/decryption operation.

(v) T_h: The running time of a SHA1 hash operation.

The authentication and key agreement phase of Li et al.'s scheme [5] requires a total of three modular exponentiation operations, one modular multiplication operation, one modular inversion operation, and four SHA1 hash operations at the HAN_{GW_i}'s side to compute $(C_1, C_2, C_3, ID_j, sk_{H-N}, C_6)$. While at the NAN_{GW_j}'s side, it requires five modular exponentiation operations, one modular multiplication operation, and four SHA1 hash operations to calculate $(ID_i, C_1, C_4, C_5, C_6, sk_{N-H})$. Therefore, Li et al.'s scheme takes around 1.0426ms and 1.6579ms at HAN_{GW_i}'s and NAN_{GW_j}'s sides respectively during the authentication and key agreement phase.

In our proposed scheme, the authentication and key agreement phase requires a total of three modular exponentiation operations, one modular multiplication operation,

Table 2: Running operations of related operations (millisecond).

	Our proposed scheme	Scheme [5]
T_{HAN-GW}	$3T_{me} + T_m + 4T_h$	$3T_{me} + T_m + T_{inv} + 4T_h$
T_{NAN-GW}	$5T_{me} + T_m + 4T_h$	$5T_{me} + T_m + 4T_h$
communication cost	$3\|G\| + 3\|h\| + \|h'\|$	$3\|G\| + 5\|h\|$

Table 3: Running times of related operations (millisecond).

	T_{HAN-GW}	T_{NAN-GW}	Communication cost
Our proposed scheme	0.9963 ms	1.6578 ms	3776 bits
Scheme [5]	1.0426 ms	1.6578 ms	3872 bits

and four SHA1 hash operations at the HAN_{GW_i}'s side to compute (A, C, S, sk_{H-N}, v). While at the NAN_{GW_j}'s side, it also requires five modular exponentiation operations, one modular multiplication operation, and four SHA1 hash operations to calculate $(A, B, ID_i', S, sk_{N-H}, v)$. Therefore, this phase only takes around 0.9963 ms and 1.6578 ms at HAN_{GW_i}'s and NAN_{GW_j}'s sides respectively.

For the communication cost, we need to transmit two elements in the group $\mathbb{G}$ (i.e., A, C) and only one element in the group Z_q^* (i.e., t_i) at the HAN_{GW_i}'s side, and there is one element in $\mathbb{G}$ (i.e., B), two elements in group Z_q^* (i.e., v, t_j) to be transmitted at the NAN_{GW_i}'s side. We assume that $|G|$ denotes the length of element in group $\mathbb{G}$ and $|h|, |h'|$ denote the length of element in group Z_q^* and $(\log_2 q + |ID|)$. Thus, the total communication cost of our proposed scheme is $3|G|+3|h|+|h'| = 3776$ bits (assume that the length of identity is 64 bits). Similarly, we note that there are three elements in $\mathbb{G}$ (i.e., C_1, C_2, C_4) and five elements in the group Z_q^* (i.e., C_3, C_5, C_6, t_i, t_j) to be transmitted over the network channel. Thus, the total communication cost of Li et a."s scheme is $3|G| + 5|h| = 3872$ bits.

As shown in Tables 2 and 3, our proposed scheme addresses the security weakness of the authentication phase without increasing the computation and communication costs when it is compared to [5]. In particular, the computation cost at the HAN-GW's side is even slightly lower than that of [5] because the proposed protocol removes the inversion operation. Therefore, our proposed protocol is more suitable for the practical deployment of the smart grid.

8. Conclusion

Device authentication and secure message transmission are important processes in the practical deployment of the smart grid. Li et al. recently proposed a lightweight message authentication scheme for the smart grid with user anonymity and they claimed it is secure. However, we found that their scheme fails to achieve device mutual authentication, which results in possible network availability attacks that include DoS attacks. To address the weaknesses in Li et al.'s scheme, we proposed an improved message authentication scheme which does not incur additional computation and communication costs. A security analysis demonstrates that our proposed scheme can satisfy various security requirements for the smart grid. Our future work will focus on reducing the communication cost during the authentication process.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request. Fully documented templates are available in the elsarticle package on CTAN.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported by the National Natural Science Foundation of China (Nos. 61772377, 61572370, 61572379) and the fund of the Guangxi Key Laboratory of Cryptography and Information Security (No. GCIS201608).

References

[1] W.-L. Chin, Y.-H. Lin, and H.-H. Chen, "A framework of machine-to-machine authentication in smart grid: a two-layer approach," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 102–107, 2016.

[2] 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*, vol. 2, no. 4, pp. 675–685, 2011.

[3] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for internet of things-based energy internet," *Future Generation Computer Systems*, 2018.

[4] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.

[5] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *Journal of Parallel and Distributed Computing*, 2017.

[6] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: classification by sources of threats," *Journal*

of Electrical Systems and Information Technology, vol. 5, no. 3, pp. 468–483, 2018.

[7] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629–640, 2014.

[8] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.

[9] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907–921, 2016.

[10] K. Mahmood, S. Ashraf Chaudhry, H. Naqvi, T. Shon, and H. Farooq Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers and Electrical Engineering*, vol. 52, pp. 114–124, 2016.

[11] N. Saxena and S. Grijalva, "Efficient signature scheme for delivering authentic control commands in the smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4323–4334, 2018.

[12] A. N. Samudrala and R. S. Blum, "Asymptotic analysis of a new low complexity encryption approach for the internet of things, smart cities and smart grid," in *Proceedings of the IEEE International Conference on Smart Grid and Smart Cities (ICSGSC '17)*, pp. 200–204, July 2017.

[13] L. Ji, L. Wang, and C. Liao, "A new method of encryption wireless energy transmission for ev in the smart grid," *CES Transactions on Electrical Machines and Systems*, vol. 1, no. 4, pp. 405–410, 2017.

[14] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.

[15] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2428–2435, 2017.

[16] B. Li, Y. Huang, Z. Liu, J. Li, Z. Tian, and S.-M. Yiu, "HybridORAM: practical oblivious cloud storage with constant bandwidth," *Journal of Information Science*, 2018.

[17] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Information Sciences*, vol. 412-413, pp. 223–241, 2017.

[18] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *Institute of Electrical and Electronics Engineers. Transactions on Computers*, vol. 65, no. 10, pp. 3184–3195, 2016.

[19] M. Wazid, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Secure three-factor user authentication scheme for renewable-energy-based smart grid environment," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3144–3153, 2017.

[20] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak, and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," *Renewable & Sustainable Energy Reviews*, vol. 54, pp. 396–405, 2016.

[21] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900–1910, 2018.

[22] T. W. Chim, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, 2015.

[23] A. C.-F. Chan and J. Zhou, "Cyber–physical device authentication for the smart grid electric vehicle ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.

[24] X. Li, J. Niu, S. Kumari, F. Wu, and K.-K. R. Choo, "A robust biometrics based three-factor authentication scheme for global mobility networks in smart city," *Future Generation Computer Systems*, vol. 83, pp. 607–618, 2018.

[25] P. Gope and T. Hwang, "Enhanced secure mutual authentication and key agreement scheme preserving user anonymity in global mobile networks," *Wireless Personal Communications*, vol. 82, no. 4, pp. 2231–2245, 2015.

[26] 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 protection for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[27] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018.

[28] D. Koo, Y. Shin, and J. Hur, "Privacy-preserving aggregation and authentication of multi-source smart meters in a smart grid system," *Applied Sciences*, vol. 7, no. 10, p. 1007, 2017.

[29] D. He, S. Zeadally, H. Wang, and Q. Liu, "Lightweight data aggregation scheme against internal attackers in smart grid using elliptic curve cryptography," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 3194845, 11 pages, 2017.

[30] J. Shen, S. Chang, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018.

[31] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[32] M. Ennahbaoui and H. Idrissi, "Zero-knowledge authentication and intrusion detection system for grid computing security," in *Information Innovation Technology in Smart Cities*, pp. 199–212, Springer, 2018.

[33] G. S. Aujla, R. Chaudhary, S. Garg, N. Kumar, and J. J. P. C. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIOT environment," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629–2640, 2018.

[34] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[35] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice-based anonymous authentication protocol for mobile devices," *IEEE Systems Journal*, pp. 1–11, 2018.

[36] C. Lin, D. He, X. Huang, K. R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, no. 1, pp. 42–52, 2018.

[37] D. He, N. Kumar, H. Wang, L. Wang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 633–645, 2018.