IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 15, 2021, accepted May 9, 2021, date of publication May 17, 2021, date of current version May 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3080835

An Ultra-Lightweight Mutual Authentication Scheme for Smart Grid Two-Way Communications

SAEED AGHAPOUR[1], MASOUD KAVEH[2], MOHAMMAD REZA MOSAVI[2], AND DIEGO MARTÍN[1]

[1]ETSI de Telecomunicación, Universidad Politécnica de Madrid, 28040 Madrid, Spain
[2]Department of Electrical Engineering, Iran University of Science and Technology, Tehran 13114-16846, Iran

Corresponding author: Diego Martín (diego.martin.de.andres@upm.es)

ABSTRACT It is well established that the efficiency, safety, flexibility, and reliability of the power grid is improved by utilization of information and communication technology (ICT) in smart grid. Nevertheless, the use of ICT introduces serious challenges regarding security issues, which has led to introducing many protocols for securing the communication between the smart meters and neighborhood gateways in recent years. However, providing functional and security features such as two-way communication and resistance against memory attack, alongside the lightweight design is the ultimate goal of these schemes. To overcome all the mentioned problems, this paper proposes a super-lightweight secure protocol based on only one-way hash functions and XOR operation, which provides two-way communication and secure one-time pad key for each data transmission. The security and performance analysis shows that not only does the proposed scheme resist the existing attacks but also it dramatically improves the efficiency in terms of storage burden and computational cost.

INDEX TERMS Mutual authentication, lightweight design, two-way communication, smart grid security.

I. INTRODUCTION

Smart grid is becoming the future of power grid by utilization of information and communication technology (ICT). ICT provides two-way information flow alongside the one-way electrical flow of the traditional power grid, making the smart grid more efficient, safer, and more reliable. Fossil fuels consumption, peak power demand, and greenhouse gases emission are the other concerns that will be solved by the smart grid. Although deploying the modern communication technologies in the smart grid adds attractive features to the traditional power grid, it definitely leads to serious new challenges in security [1]–[3].

Due to the importance of the secrecy of personal data, security has to be studied carefully from various perspectives in smart grid. For example, an adversary can acquire the transmitted message and obtain the vital data of the private life of customers, or send altered/replayed messages to utility service providers leading them to make the wrong decisions.

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

In another type of attack, a smart meter's (SM) memory may be altered by the adversary or even by a consumer who wants to use the energy without paying, hence, the system should resist memory modification attack as well as the cyber-attacks [4]–[6].

A. SMART GRID SYSTEM MODEL

As illustrated in Figure 1, smart grid has a hierarchical communication model. A home area network (HAN) as the first communication level consists of one SM and some smart appliances. Every SM is installed in open and collects data from the smart appliances in the HAN. Furthermore, the SMs are considered extremely resource-constrained devices. HAN includes the consumers in the overall power system model. In the second level at the neighborhood area network (NAN), the neighborhood gateway (NG) periodically collects the electricity reports from several hundreds of SMs and then checks their authenticity, confidentiality, and integrity. NAN can be equivalent to the power distribution in smart grid power system layer. Finally, at the top level, the management and control center collects the energy consumption reports

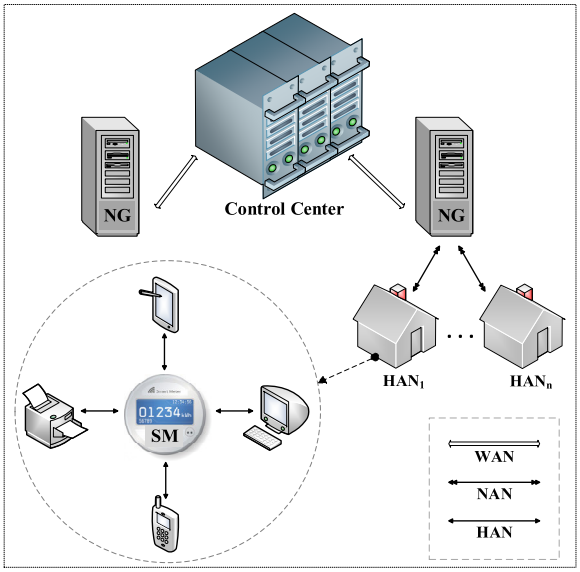

FIGURE 1. The smart grid communication model.

from the NGs in the wide area network (WAN) and based on that makes the final decisions. WAN can be also considered equivalent to the power transmission and generation in smart grid power system layer [1]. The concentration of this paper is based on communications between the SMs and NG in the NAN environment.

B. THREAT MODEL

The threat model on the *NAN* communication system network in this paper follows the Dolev and Yao (DY) [7] model and is considered as follows: An adversary has full access to the channel and can eavesdrop the transmission packets and try to decrypt the packets to obtain the data reports or control messages. Besides that, the adversary can perform man in the middle attack and try to alter or replay the communicated messages between *SM*s and *NG*. The adversary can also consume *SM*s' and *NG*'s resources by applying DoS attack. Furthermore, since *SM*s are located in the open, the adversary or even a *HAN* consumer can alter the *SM*s' memory. In the rest of this paper, we show how the proposed scheme can resist against the mentioned attacks.

C. RELATED WORKS

Many security schemes have been introduced in recent years, which have proposed different communication protocols between the SMs and NG [8]–[16]. In 2011, Fouda *et al.* [8] proposed a message authentication scheme features as a basic yet crucial component for secure smart grid communication. In their proposed scheme, the mutual authentication has been provided and the shared session key with Diffie-Hellman key exchange protocol has been established. The provided security and performance analysis showed that their scheme could fulfill the desirable security requirements as well as the efficiency terms. Mahmood *et al.* [9] presented a message authentication scheme for smart grid communications in power sector. They used the hybrid Diffie-Hellman-based authentication scheme using advanced encryption standard (AES) and Rivest-Shamir-Adleman (RSA) for session key generation. The hash-based message authentication code is also exploited for ensuring message integrity. Their scheme provided mutual authentication, the replay and man-in-the-middle attacks resistance, and achieved message integrity, but increasing overall communication and computational overheads. After then, Uludag *et al.* [10] proposed a secure and scalable data collection with time minimization in smart grid. Alongside the formal security analysis, they presented some optimization solutions for minimizing the total data collection time.

In 2014, Li *et al.* [11] used Merkle hash tree and AES to establish secure communication between the SM and NG. They showed that not only their scheme is secure against message analysis, message modification, replay, and impersonation attacks but also it improves communication and computational costs in comparison with RSA. Liu *et al.* [12] proposed a secure communication scheme based on the Lagrange polynomial for the NAN communication in 2016. They showed that their scheme is secure against the security attacks, as well as providing better performance in comparison with Li *et al.* [11]. Abbasinezhad-Mood and Nikooghadam [13] proposed an ultra-lightweight communication scheme based on logical XOR operation, pseudo random number generation (PRNG), and one-way hash function in 2018. They showed that compare to previous schemes not only their scheme has better security claims but also it performed better than schemes [11] and [12] in terms of storage, communication, and computational costs. Quite recently in 2020, Kaveh *et al.* presented a mutual authentication scheme based on physically unclonable function (PUF) for NAN communication system of the smart grid [14]. In the proposed scheme, a PUF-based one-time pad key has been deployed that leads to increasing the security of the system against brute-force and physical attacks. Furthermore, they showed that their scheme outperforms the state-of-the-art in terms of storage burden and computational cost. Garg *et al.* [15] proposed a secure authentication scheme for smart metering infrastructure in smart grid in 2019 based on Fully Hashed Menezes-Qu-Vanstone key exchange scheme along with Elliptic Curve cryptosystem (ECC) and one-way hash functions. They showed that their scheme provides trust, anonymity, and mutual authentication, with reduced energy, communication, and computational overheads for resource-constrained SMs. Recently in 2020, Sureshkumar *et al.* [16] proposed a mutually authenticated key agreement scheme between the SMs and NG by which NG can initiate the communication. Their proposed protocol has been proven to be secure using the formal methods Gong, Needham, and Yahalom logic, and the automated ProVerif tool. They could also provide excellent security features as well as efficient performance overhead.

Although the proposed schemes in [11]–[16] have improved some of the security and efficiency issues, all of them lack in one or more important features. One of those features is updating the stored cryptographic key which is usually used for a long time. The other feature is enabling secure two-way communication in each time interval of data transmission that is an essential part of the smart grid. Last but not least is to designing the proposed protocol in a lightweight manner to impose less overheads not only on the SM side but also on the NG side. Therefore, this paper is going to propose a novel and ultra-lightweight protocol to provide the mentioned interesting features for the smart grid. Some of these features are listed in Table 7.

D. PAPER CONTRIBUTION

This paper aims to overcome the mentioned drawbacks of the former schemes presented in [8]–[14], by proposing a super-lightweight authentication scheme for the smart grid NAN communication system. The key contributions of this paper are summarized as follows:

- A novel lightweight security protocol based on only one-way hash function and logical XOR which can resist the possible attacks in the smart grid NAN environment including message analysis, impersonation, message altering, replay, denial of service (DoS), and SM memory modification attack.
- Providing two-way communication alongside the mutual authentication for each time interval of data transmission.
- Enabling a one-time pad key cryptosystem, which provides better security features.
- Super-lightweight design of the proposed scheme that enhances the efficiency of resource consumptions of both SM and NG sides in comparison with the state-of-the-art. Therefore, this feature alongside the formal security analysis can lead to practical deployment of the proposed scheme in near future communication of smart grid.

E. PAPER ORGANIZATION

The remainder of this paper is organized as follows. The proposed scheme for the NAN communication system is detailed in section II. Section III analyzes the security of the proposed protocol while section IV provides a formal security analysis. A comparative performance evaluation is presented in section V and finally, the conclusion of this paper is drawn in section VI.

II. THE PROPOSED AUTHENTICATION SCHEME

In this section, we introduce the proposed lightweight authentication protocol (see figure 2). Furthermore, the used notations and their corresponding meanings in this section are presented in Table 1.

A. SECURE INSTALLATION STAGE

In this stage, each smart meter SM_j registers itself to NG and a secret random initial key K_0^j is allocated and sent to them by NG through a secure channel. Afterward, for $j = 1, 2, \ldots, l$, NG stores (ID_j, K_0^j) in its database and each SM_j will store the initial cryptographic key K_0^j in its memory. Note that, although this assumption can be considered a strong one, this stage happens only once in the initialization when smart meters want to join the network.

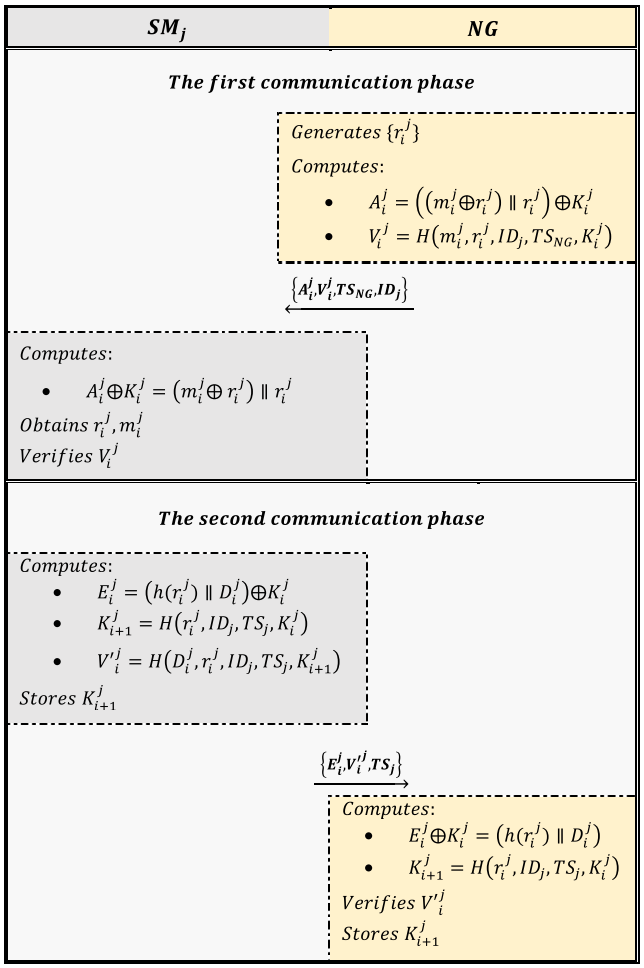

FIGURE 2. The proposed protocol.

B. SECURE COMMUNICATION STAGE

In order for smart meters to send their messages to NG in an authenticated manner through an insecure channel, SM_j performs the following steps:

Figure 2 shows the proposed mutual authentication protocol. The communication stage of the proposed scheme consists of two communication phases. The communication from NG to SM_j resulting in authentication of NG's control message and the communication from SM_j to NG which results in authentication of SM_j's data reports. The first authentication phase starts by NG applying the following steps:

- Generates a random number r_i^j.
- Searches its memory to find the corresponding communication key K_i^j for ID_j.

TABLE 1. Notations and their meanings.

Symbol	Description
$h(.)$	The 16B one-way hash function
$H(.)$	The 32B one-way hash function
SM_j	jth smart meter
NG	Neighborhood gateway
ID_j	Identifier of SM_j
TS_j	Timestamp of SM_j
TS_{NG}	Timestamp of NG
K_i^j	The ith communication key
j	jth smart meter
i	ith time interval of data transmission
ms	Millisecond
KB	Kilo byte
$\oplus$	The XOR operator
$\|\|$	The concatenation operator
$\|X\|$	The size of parameter X
X^*	The forged parameter of X
l	Number of smart meters

- Computes $A_i^j = \left(\left(m_i^j \oplus r_i^j\right) \| r_i^j\right) \oplus K_i^j$ as the encrypted message.
- Computes the verifier $V_i^j = H\left(m_i^j, r_i^j, ID_j, TS_{NG}, K_i^j\right)$.
- Sends $\left\{A_i^j, V_i^j, TS_{NG}, ID_j\right\}$ to SM_j.

After receiving the packet from NG, each SM_j obtains r_i^j and m_i^j by computing $A_i^j \oplus K_i^j$. Furthermore, in order to verify the authenticity of NG's packet, SM_j verifies V_i^j by computing $V_i^j = H\left(m_i^j, r_i^j, ID_j, TS_{NG}, K_i^j\right)$. Hence, if the verification of V_i^j fails, SM_j finds out that some of the parameters have been altered by an adversary and discards the received packet and stops the protocol. Otherwise, the authenticity of NG is verified by SM_j and the first authentication phase ends.

As for the second authentication phase, the following steps are performed: First SM_j acts as follows:

- Computes $E_i^j = \left(h(r_i^j) \| D_i^j\right) \oplus K_i^j$ as the encrypted message.
- Creates $K_{i+1}^j = H\left(r_i^j, ID_j, TS_j, K_i^j\right)$ as the new cryptographic key.
- Computes $V'^j_i = H\left(D_i^j, r_i^j, ID_j, TS_j, K_{i+1}^j\right)$ as its verifier.
- Sends $\left\{E_i^j, V_i'^j, TS_j\right\}$ to NG.
- Replaces the old cryptographic key K_i^j with K_{i+1}^j in its memory storage as the new cryptographic key.

After receiving the packet, NG decrypts E_i^j by computing $E_i^j \oplus K_i^j$ and $h(r_i^j)$ to obtain the data report D_i^j from the corresponding smart meter. To authenticate SM_j's data report, NG creates the key $K_{i+1}^j = H\left(r_i^j, ID_j, TS_j, K_i^j\right)$ and uses it to compute $H\left(D_i^j, r_i^j, ID_j, TS_j, K_{i+1}^j\right)$. Then, NG checks $H\left(D_i^j, r_i^j, ID_j, TS_j, K_{i+1}^j\right)$ with the received V_j' to verify the validity of the obtained data report.

Now, if the verification fails in any way, NG rejects the authentication request and discards the received packet. Using the next key K_{i+1}^j in the verifier ensures the smart meters and NG that they are able to decrypt the next communication messages. In other words, if the verification process of $V_i'^j$ fails, NG requests SM_j to send their packet again and will not stop until the verification process passes. By doing this NG makes sure that his next encrypted control message can be decrypted by SM_j. When the process verification successes, NG acts as follow:

- Compares the decrypted message, D_i^j, with the existing report format and only if it is in the certain predefined format, accepts it otherwise, rejects it.
- Replaces $\left(ID_j, S_i^{NG}\right)$ with the new pair (ID_j, S_{i+1}^{NG}) in its database. The second authentication phase ends here.

It goes without saying, that in order to be able to apply XOR operation, all of the involving parties in the XOR operands should be of the same length. In this paper, 32 bits length for ID_j and TS, 128 bits for D_i^j, r_i^j, and m_i, and 256 bits for key K_i^j is considered. Also, we consider $h()$ and $H()$ are two one-way collision-resistant hash function which get inputs with arbitrary length and outputs 16 B and 32 B, respectively.

It is worth noting, that the collision-resistant property of the cryptographic hash functions and the existence of timestamps in V_i^j, K_i^j, and $V_i'^j$ ensures data freshness and secures the scheme from replay attacks. Besides that, the idea of using a random number r_i^j in creating the cryptographic key is to change the key in each communication interval meaning that each cryptographic key is used once which improves the security of the proposed scheme against memory modification attack. Hence, the two important security properties of the key that are having a long length of 256 bits and one time usage, provides a significant level of security.

III. INFORMAL SECURITY DISCUSSION

In this section, after introducing the threat model, we discuss the security of the proposed scheme against possible attacks including message analysis, message altering, message injection, replay, memory modification and DoS attack with details. Furthermore, we consider that the mentioned attacks are performed by probabilistic a polynomial time (PPT) adversary.

A. RESISTANCE AGAINST MESSAGE ALTERING AND INJECTION ATTACK

In these kind of attacks, an adversary can impersonate and act as either one of the NG or SM_j. It is considered that by eavesdropping, adversaries have access to transmitted packets. Hence, their goal is to act as one of the involved parties

of the protocol and change the transmitted packet in such a way that the other party verifies and as a result authenticates them. In this type of attack based on whom an adversary wants to impersonate we consider two scenarios: first, when the adversary impersonates *NG* and wants to authenticate its message to *SM* and second, when the adversary impersonates SM_j and wants to authenticate its message to *NG*.

In the first scenario, the adversary has A_i^j and wants to create A_i^{*j} and the corresponding verifier V_{ij}^* for its message m_i^* in such a way to pass the verification process on *SM*'s side. In other words, by having $A_i^j = \left(\left(m_i^j \oplus r_i^j\right) \parallel r_i^j\right) \oplus K_i^j$ the adversary's goal is to create $A_i^{*j} = \left(\left(m_i^{*j} \oplus r_i^j\right) \parallel r_i^j\right) \oplus K_i^j$ and the verifier $V_{ij}^* = H\left(m_i^{*j}, r_i^j, ID_j, TS_{NG}, K_i^j\right)$. However, because of the secrecy of the cryptographic key K_i^j and the one-way collision-resistant property of the hash functions, this attack is not feasible for PPT adversaries.

As for the second scenario, where the adversary acts as SM_j, he has access to E_i^j, A_i^j, and his goal is to change the message D_i^j to D_i^{*j} and creates the new encrypted message $E_i^{*j} = \left(h(r_i^j) \parallel D_i^{*j}\right) \oplus K_i^j$ and the corresponding verifier $V_{ij}^{*'} = H\left(D_i^{*j}, r_i^j, ID_j, TS_j, K_{i+1}^j\right)$ and send it to *NG* with the hope of passing the verification process in *NG*'s side. However, similar to the first scenario because of the secrecy of the key and the collision-resistant property of the hash function, the attack is not feasible.

B. RESISTACNE TO MESSAGE ANALYSIS ATTACK

In this attack, an adversary tries to decrypt the transmitted packets and extract the messages. In other words, the adversary's goal is to decrypt A_i^j or E_i^j to obtain the message m_i or the data report D_i^j The best an adversary can do is that instead of attacking the key 256 bits K_i^j by brute force, use transmitted messages and by applying some operations on them achieve m_i^j or D_i^j. As a result, the adversary's goal reduces to obtain m_i or D_i^j from $A_i^j = \left(\left(m_i^j \oplus r_i^j\right) \parallel r_i^j\right) \oplus K_i^j$ and $E_i^j = \left(h(r_i^j) \parallel D_i^j\right) \oplus K_i^j$. However, the existence of $h(r_i^j)$ in E_i^j and the random number r_i^j in both A_i^j, E_i^j makes it impossible for the adversary to obtain any information on the messages. Also, since the random number r_i^j hence the communication key K_i^j changes for each communication, the attacker cannot use the forward leaked information to decrypt former messages. As a result, the proposed scheme is secure against message analysis attacks.

C. RESISTANCE TO REPLAY ATTACK

In this attack, an adversary stores former transmitted messages and wants to use them in future communications. In this attack, the probability of success of PPT adversary for this attack is equal to the case when $V_i^j = V_l^j$ which i is a former time interval and t is the time interval when the adversary wants to attack the protocol. Hence, the probability of success reduces to when $H\left(m_i^j, r_i^j, ID_j, TS_{NG}, K_i^j\right) = H(m_t^j, r_t^j, ID_j, TS_{NG}, K_t^j)$ holds. However, as mentioned before, because of the presence of *TS* in the message verifiers, one time pad feature of the cryptographic key K_i^j, and creation of fresh random number r_i^j for each communication interval the probability of adversary's success is equal to find a collision in the hash function which is negligible. Similarly, the same analysis can be presented for $V_i^{'j}$.

D. RESISTANCE TO MEMORY MODIFICATION ATTACK

This attack happens when an adversary gets access to one of the smart meters' memory storage and wants to change it meaningfully in such a way that the communication continues and also SM_j and *NG* not be able to detect the change. In other words, we assume that an adversary does not want to retrieve the key but to change it only. Hence, by attacking the SM_j's memory storage the adversary can change the value K_i^j to $K_i^{*j} = K_i^j \oplus X$ without retrieving the key. The parameter X is 256 bits long and is chosen by an adversary in any way he/she sees fit. However, in the first authentication phase when SM_j wants to authenticate *NG*'s control message it checks if the equation $V_i^j = H\left(m_i^j, r_i^j, ID_j, TS_{NG}, K_i^{*j}\right)$ holds or not. However, the probability that the equation $H(m_i^j, r_i^j, ID_j, TS_{NG}, K_i^j) = H\left(m_i^j, r_i^j, ID_j, TS_{NG}, K_i^j \oplus X\right)$ holds is equal to finding a collision in the hash function, which is negligible for *PPT* adversaries. Hence, the attack is not practical.

E. RESISTACNE TO DoS ATTACK

In this attack, we investigate the computational standpoint of DoS attack. In other words, we consider the case when an adversary tries to overload the system by sending redundant bogus messages to the involved parties of the protocol in an attempt to force them to use unnecessary computations and store futile messages to prevent them from receiving the authentic messages. In this model, the attacker can act as either one of the *NG* or SM_j. In the scenario where the attacker acts as *NG*, it sends a lot of arbitrary pair messages like $\{X, Y, Z, TS\}$ instead of $\left\{A_i^j, V_i^j, ID_j, TS\right\}$ to SM_j (first communication phase). However, as it is shown in section II, the verification process in SM_j is done by only executing two *XOR* operations and one hash function, which are insignificant even with SM_j's standards. Hence, SM_j does not need to store these fake messages in its buffer and rejects them instantly.

As for the second scenario where the attacker impersonates SM_j, the adversary sends fake packets $\{X, Y, TS\}$ instead of the authentic messages $\{E_i^j, V_{ij}^{'}, TS\}$ and forcing *NG* to compute one *XOR* operations and three hash functions. Needless to say, this computational overhead is negligible in comparison with *NG*'s computational power. Therefore, *NG* rejects these kinds of bogus messages immediately without the need

of buffering them. As a result, a DoS attack is not feasible in the proposed protocol.

F. FORWARD SECRECY

Forward secrecy means that even if one of the session keys has been exposed, the former session keys which have been used to encrypt the communicated messages must not be exposed. In this part, because of using random numbers, we show that our scheme has forward secrecy. Consider that we are at the i+1-th round and the i-th key has been exposed. As shown in the protocol, the i-th key is calculated as $K_i^j = H(r_{i-1}^j, ID_j, TS_j, K_{i-1}^j)$ and is used only once. The goal of adversary is to compute $K_l^j = H(r_{l-1}^j, ID_j, TS_j, K_{l-1}^j)$ where $l < i$. In other words, the adversary must be able to compute $H(r_{l-1}^j, ID_j, TS_j, K_{l-1}^j)$ by having $H(r_{i-1}^j, ID_j, TS_j, K_{i-1}^j)$, ID_j and TS_j. However, because of the secrecy of r_{l-1}^j and K_{l-1}^j, the chances of adversaries success is equal to finding a collision in the one-way hash function, which is computationally infeasible.

IV. FORMAL SECURITY ANALYSIS

In this section, we bring a formal proof to make sure that any adversary as claimed in section III cannot achieve the communicated secret parameters of the protocol. For this matter, Mao and Boyd logic [21], which is an improved version of BAN logic [22], is used. Therefore, the goal of this section is to prove that in the proposed scheme r_i^j, m_i^j, and D_i^j are good-shared secrets between SM_j and NG.

According to [21], in order to setup the proof, it is needed to first idealize the protocol and define some initial and beliefs. In addition, in Mao and Boyd logic, hashed values are considered not alterable hence; they do not appear in idealized form. Note that all of the used notations in this section are derived from [21]. The basics of Mao and Boyed logic has been presented in the Appendix section. Now, the idealized form of the messages in our protocol is as follow:

1. $NG \rightarrow SM_j : \left\{ r_i^j \,\Re\, m_i^j \,\Re\, TS_{NG} \right\}_{K_i^j}$
2. $SM_j \rightarrow NG : \left\{ D_i^j \,\Re\, r_i^j \,\Re\, TS_{SM_j} \right\}_{K_i^j}$

The initial beliefs for the proposed protocol are as follow:

1. $SM_j \mid\equiv SM_j \overset{K_i^j}{\leftrightarrow} NG$ and $NG \mid\equiv SM_j \overset{K_i^j}{\leftrightarrow} NG$. As K_0^j is securely shared between SM_j and NG.
2. $SM_j \mid\equiv \{NG\}^c \triangleleft \left|\left| D_i^j \right|\right.$ and $NG \mid\equiv SM_j \mid\equiv \{NG\}^c \triangleleft \left|\left| D_i^j \right|\right.$ as SM_j securely generates D_i^j.
3. $SM_j \mid\overset{k_i^j}{\sim} D_i^j$. Message two in the idealized protocol.
4. $SM_j \mid\equiv \#(D_i^j)$ and $SM_j \mid\equiv \#(TS_j)$, Since SM_j generates D_i^j each time and TS_j is its fresh timestamp.
5. $NG \mid\equiv \#(r_i^j)$ and $NG \mid\equiv \#(m_i^j)$, Since NG generates r_i^j and m_i^j in each run of the protocol.
6. $NG \mid\equiv Sup(SM_j)$ and $SM_j \mid\equiv Sup(NG)$. SM_j and NG are the super principal of each other with-respect-to messages one and two in the idealized protocol.
7. $SM_j \overset{K_i^j}{\triangleleft} r_i^j \Re\, TS_{NG}$ and $SM_j \overset{K_i^j}{\triangleleft} m_i^j \Re\, TS_{NG}$. Message one in the idealized protocol.
8. $NG \overset{K_i^j}{\triangleleft} D_i^j \Re\, r_i^j$ and $NG \overset{K_i^j}{\triangleleft} r_i^j \Re\, TS_j$. Message two in the idealized protocol.
9. $NG \mid\equiv \left\{SM_j\right\}^c \triangleleft \left|\left| r_i^j, m_i^j \right|\right.$ and also $SM_j \mid\equiv NG \mid\equiv \left\{SM_j\right\}^c \triangleleft \left|\left| r_i^j, m_i^j \right|\right.$. Because NG securely generates r_i^j and m_i^j in each run of the protocol.
10. $NG \mid\overset{k_i^j}{\sim} r_i^j$ and $NG \mid\overset{k_i^j}{\sim} m_i^j$. Message one in the idealized form.

Figure 3 demonstrates details of the formal proof for the proposed scheme, which consists of four tableaux where each of them is a proof for one of the secret parameters. For example, the tableau of Figure 3(a) shows that SM believes D_i^j is a good-shared secret between SM and NG ($SM \mid\equiv SM \overset{D_i^j}{\leftrightarrow} NG$). To prove that, by using the Good-Key Rule [21] the problem reduces to showing that in SM's opinion the data is fresh ($SM \mid\equiv \#(D_i^j)$) and no one except SM and NG can see it ($SM \mid\equiv \{NG, SM\}^c \triangleleft \left|\left| D_i^j \right|\right.$). Needless to say, because SM creates D_i^j, its freshness is well known by him. For proving $SM \mid\equiv \{NG, SM\}^c \triangleleft \left|\left| D_i^j \right|\right.$ by using the Confidentiality Rule [21] we have to show that SM must make sure that first, no one else except it and NG knows the communication key ($SM \mid\equiv SM \overset{K_i^j}{\leftrightarrow} NG$ based on belief 1), second, only NG has access to the report message ($SM \mid\equiv \{NG\}^c \triangleleft \left|\left| D_i^j \right|\right.$ based on belief 2), and third, SM has encrypted D_i^j ($SM \mid\overset{K_i^j}{\sim} D_i^j$ based on belief 3).

As a result, the statement $SM \mid\equiv SM \overset{D_i^j}{\leftrightarrow} NG$ is valid. Furthermore, by using the initial beliefs in this section and inference rules in [21] such as Good-Key Rule, Super-Principal Rule, Freshness Rule, Confidentiality Rule, Derived Rule, Intuitive Rule, Authentication Rule, and Nonce-Verification Rule, the other claimed statements can be proved. In Figure 3, tableau b, c, and d demonstrate the proofs for statements $NG \mid\equiv SM \overset{r_i^j}{\leftrightarrow} NG$, $NG \mid\equiv SM \overset{D_i^j}{\leftrightarrow} NG$, and $SM \mid\equiv SM \overset{r_i^j}{\leftrightarrow} NG$, respectively. Needless to say, based on the idealized protocol the same proof that was provided for r_i^j can be applied on m_i^j. As mentioned before, the goal of formal proof is to prove that the communicated secret parameters (r_i^j, m_i^j, D_i^j) would remain unexposed even after the communication is over.

V. COMPARATIVE PERFORMANCE EVALUATION

This section evaluates the performance of the proposed protocol in terms of storage burden, communication overhead, and

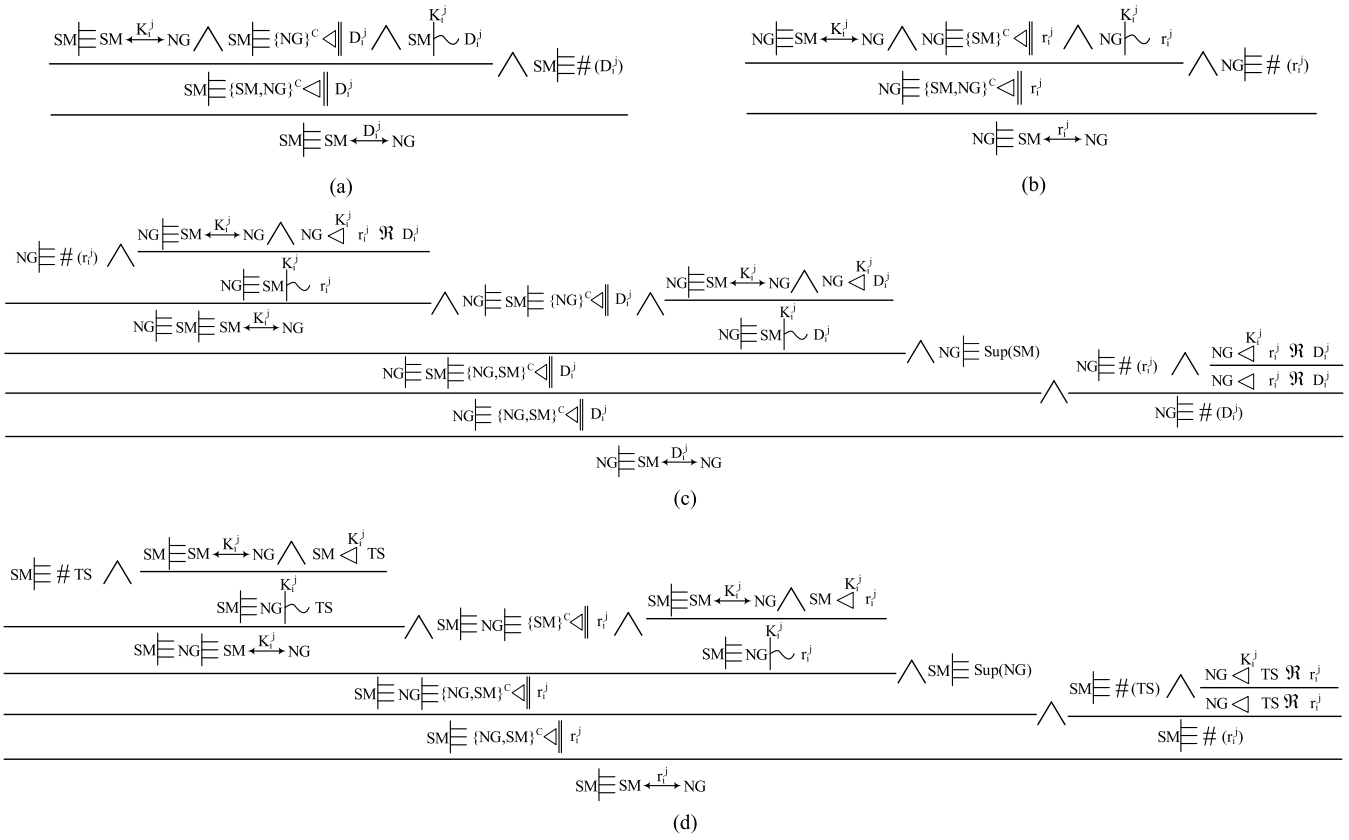

FIGURE 3. Formal security proofs for the proposed protocol: a) Proof of "SM believes D_i^j is a good-shared secret of SM and NG", b) Proof of "NG believes r_i^j is a good-shared secret of SM and NG", c) Proof of "NG believes D_i^j is a good-shared secret of SM and NG", and d) Proof of "SM believes r_i^j is a good-shared secret of SM and NG".

computational cost, and compares it with the other existing schemes proposed in [8]–[16]. In this paper, SHA-256 and a 128-bit pseudo random number generator are used to execute the cryptographic hash function and generate the pseudo-random numbers, respectively. To have a comprehensive comparison with the schemes proposed in [8]–[16], the time interval of report messages collection and communication is considered fifteen minutes. Furthermore, in order to have a practical evaluation, we analyze and compare the performance of the schemes for various values of time intervals from one minute to fifteen minutes. The performance analysis details of the proposed protocol are shown in the following subsections.

A. STORAGE BURDEN

In this section, *NG* is assumed as a server equipped with a database with high storage capacity therefore, only the storage burden on *SM*'s side is studied. As mentioned in section II, for each protocol execution, *SM* only needs to store the 256-bit secret value (key) K_i^{SM} in its memory. Therefore, the total storage burden of the proposed scheme is 256 bit. Table 2 shows the storage cost comparison between our proposed protocol in this paper and the proposed schemes in [11]–[14]. According to Table 2, our protocol alongside

TABLE 2. Comparison of needed storage space for time interval of fifteen minutes.

Scheme [11]	Scheme [12]	Scheme [13]	Scheme [14]	Ours
34 KB	10.5 KB	0.5 KB	None	0.25 KB

presented schemes in [13] and [14] has a far better performance than the proposed schemes in [11] and [12]. In addition, Figure 4 demonstrates the storage burden of different schemes for different time intervals from one minute to fifteen minutes. According to Figure 4, the changing of time interval does not affect the storage burden of our scheme, as same as the proposed schemes in [14].

B. COMMUNICATION OVERHEAD

In the proposed protocol, the communication cost for *SM* to *NG* transmission is equal to $|TS_j| + |E_i^j| + |V'^j_i|$ and for the *NG* to *SM* is equal to $|ID_j| + |TS_{NG}| + |A_i^j| + |V_i^j|$ in which $|X|$ denotes the size of the parameter X. Hence, The overall communication overhead will be sum of the two overheads, and with time interval of fifteen minutes, in one day will be $((256 \times 4) + (32 \times 3)) \times 96 = 13.125\ KB$. One should notice that the length of time stamp and *ID*s have been considered as 8 *KB*.

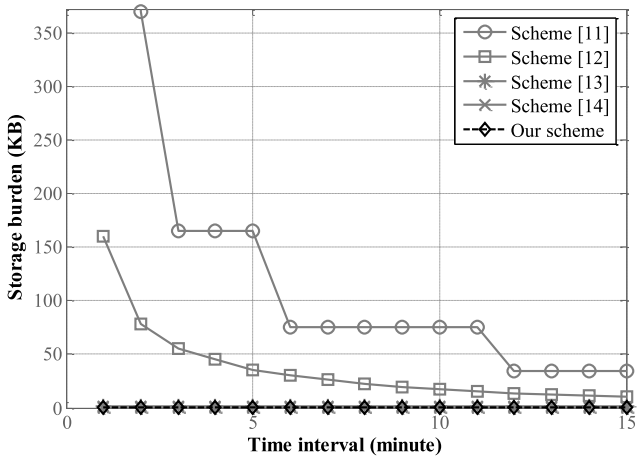

FIGURE 4. Storage burden comparison for the time intervals of one minute to fifteen minutes.

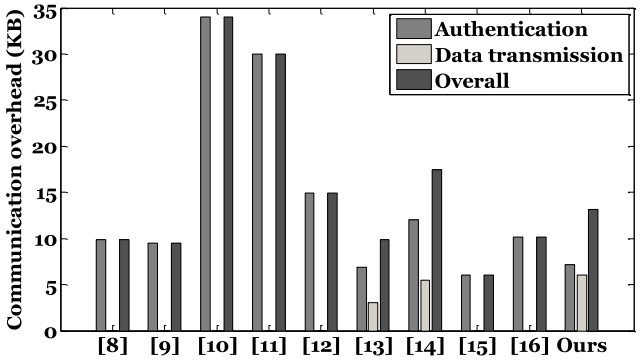

FIGURE 5. Daily communication overhead comparison for time interval of fifteen minutes.

In Figure 5, the daily communication overhead of our protocol and the proposed schemes in [8]–[16] are compared for the time interval of fifteen minutes. As seen in Figure 5, the proposed protocol in this paper has a moderate performance in this term, since it is the only protocol that provides two-way communication and mutual authentication for each time interval of data transmission, which naturally leads to increasing the communication overhead. Therefore, to have a more comprehensive comparison, we divided the communication overhead into two parts, the authentication phase and data transmission phase. $|E_i^j|$ and $|A_i^j|$ show the communication overhead for the data transmission phase. Thus, the total communication overhead for authentication and data transmission phases are 7.125 *KB* and 6 *KB*, respectively. Figure 6 depicts the total daily communication overhead of our protocol in comparison with the proposed schemes in [8]–[16] for the time intervals of one minute to fifteen minutes.

C. COMPUTATIONAL COST

In this section, the computational overhead for both *SM* and *NG* sides is studied. To that end, ArduinoLibs [23] is used

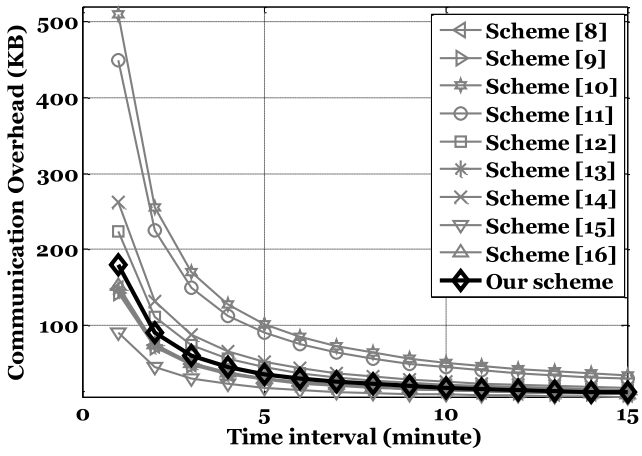

FIGURE 6. Daily communication overheads for different time intervals from one minute to fifteen minutes.

TABLE 3. Execution time of cryptographic operations on AT91SAM 3 × 8 E.

Cryptographic Operation	Execution Time
AES-256 EBC Encryption	148.8 μs
AES-256 EBC Decryption	260 μs
AES-256 EBC Key Setup	49.68 μs
SHA-256	18.4 μs
HMAC Key Setup	80.44 μs
Polynomial Generation	10 ms
Pseudo Random Number Generation	80 μs
RSA Signature Verification	34 ms
ECC Point Multiplication	3.1 ms
128-bit Arbiter PUF	82.8 μs

TABLE 4. Execution time of cryptographic operations on intel ® core™i7.

Cryptographic Operation	Execution Time
AES-256 EBC Encryption	31.7 μs
AES-256 EBC Decryption	54.4 μs
AES-256 EBC Key Setup	12.4 μs
SHA-256	10.2 μs
HMAC Key Setup	31.9 μs
Polynomial Generation	3.6 ms
Pseudo Random Number Generation	29.8 μs
RSA Signature Generation	9.8 ms
ECC Point Multiplication	1.1 ms

as the cryptographic library, and the cryptographic primitives are implemented on AT91SAM 3 × 8 E (ARM Cortex-M3 microcontroller) for measuring the computational cost on *SM* side. This microcontroller has 512 kB flash memory, 96 kB SRAM, and clock speed of 84 MHz, which is very similar to real-life smart meters [24]. Furthermore, for

TABLE 5. Daily computational cost on SM side for time interval of fifteen minutes.

Cost	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	Ours
T_h	–	–	96	255	96	200	288	384	384	384
T_{HAMC}	96	96	–	–	–	–	–	–	–	–
T_{Enc}	96	96	96	129	96	–	–	–	–	–
T_{Dec}	4	4	4	–	1	–	–	–	–	–
T_{RNG}	–	–	–	128	96	96	96	–	–	–
T_{Pol}	–	–	–	–	1	–	–	–	–	–
T_{Ver}	–	–	4	–	–	–	–	–	–	–
T_{ECC}	–	–	–	–	–	–	–	192	192	–
T_{PUF}	–	–	–	–	–	–	192	–	–	–
Total (ms)	29.78	29.78	158.06	81.07	44.77	12.36	29.02	602.26	602.26	7.06

TABLE 6. Daily computational cost on NG side for time interval of fifteen minutes.

Cost	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	Ours
T_h	–	–	96	255	96	400	288	384	384	288
T_{HAMC}	96	96	–	–	–	–	–	–	–	–
T_{Enc}	4	4	4	–	1	–	–	–	–	–
T_{Dec}	96	96	96	129	–	–	–	–	–	–
T_{RNG}	–	–	–	–	96	96	192	–	–	96
T_{Pol}	–	–	–	–	1	–	–	–	–	–
T_{Sign}	–	–	4	–	–	–	–	–	–	–
T_{ECC}	–	–	–	–	–	–	–	192	192	–
Total (ms)	9.65	9.65	46.66	11.22	7.48	6.94	8.66	215.12	215.12	5.79

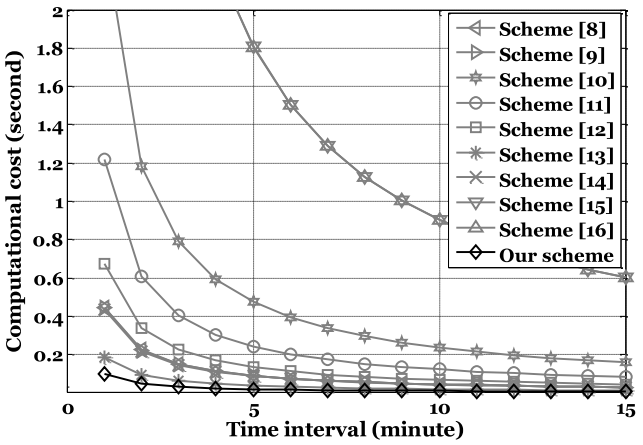

FIGURE 7. Daily computational cost comparison for SM for different time intervals.

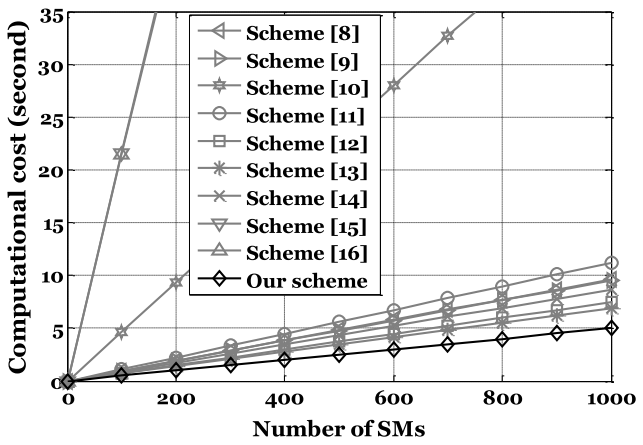

FIGURE 8. Daily computational cost comparison for NG for different number of SMs.

computing the execution times for *NG*, the cryptographic operations have been conducted on a 64-bit operating system with processor Intel® Core™i7-3612QM CPU @2.10 GHz and 6 GB (5.86 GB usable) RAM. Tables 3 and 4 show the execution time of the cryptographic operations for *SM* and *NG*, respectively.

TABLE 7. Important features of the proposed scheme in comparison with other methods.

	Message confidentiality	Message integrity	Mutual authentication	Replay attack resistance	Memory attack resistance	DoS attack resistance	Near real-time authentication	Forward secrecy	Formal proof	One-time pad key	Super-lightweight design	Two-way communication
Uludag et al.'s scheme [8]	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗
Fouda et al.'s scheme [9]	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗
Mahmood et al.'s scheme [10]	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗
Li et al.'s scheme [11]	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗
Liu et al.'s scheme [12]	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
Abbasinezhad-Mood et al.'s scheme [13]	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗
Kaveh et al.'s scheme [14]	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗
Garg et al.'s scheme [15]	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗
Sureshkumar et al.'s scheme [16]	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗
The proposed scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The number of performing various cryptographic operators by each scheme in one day is presented in Tables 5 and 6, where, T_h, T_{HAMC}, T_{Enc}, T_{Dec}, T_{RNG}, T_{Pol}, T_{Ver}, T_{ECC}, T_{Gen}, and T_{PUF} represent the execution time of one-way hash function, HMAC operation, AES encryption and decryption, pseudo-random number generation, polynomial generation, signature verification, ECC point multiplication, signature generation, and 128-bit Arbiter PUF, respectively. In our scheme, SM_j only needs to perform four one-way hash function for verifying V_i^j, creating K_{i+1}^j, creating $h(V_i^j)$, and generating V'^j_i in each run of the protocol. As a result, for one day of communication with a time interval of fifteen minutes, the total computational cost is $(96 \times 4 \times 18.4\mu s) \approx 7.06\, ms$. At the other side, *NG* needs to execute three one-way hash functions and one PRNG in each protocol execution. Tables 5 and 6 compares the computational cost of our protocol with the proposed schemes in [8]–[16] for both SM and NG sides. Even though our protocol is the only one among the other mentioned schemes applying mutual authentication and two-way communication in each protocol execution, it still has the lowest computational overhead for both sides of *SM* and *NG*. As mentioned before, by technology advancement resulting in an increase of the computational power of computers, a shorter updating period of the cryptographic keys is needed. As a result, the proposed schemes in [8]–[16] have to run their key establishment protocol faster, which consequently leads to an exponential rise in computational overhead. Figure 7 depicts the computational cost comparison between the mentioned schemes for different time intervals from one minute to fifteen minutes on the *SM*s' side. The daily computational cost of *NG* is shown in Figure 8 based on different connected *SM*s in the network (for the time interval of fifteen minute). Furthermore, a feature-based comparison between the proposed scheme and other existing schemes is shown in Table 7.

VI. CONCLUSION AND FUTURE WORK

This paper has proposed a novel authentication protocol for smart grid *NAN* communications, which only uses lightweight cryptographic operations, i.e. one-way hash function and logical XOR. Our proposed scheme not only provides one-time pad fresh key for each communication but also adds other important features like mutual authentication and two-way communication. Furthermore, the security analyses and formal proof show that the proposed scheme is secure against the mentioned possible attacks. Besides that, the performance evaluations demonstrate that the proposed scheme has great efficiency in terms of computational cost and storage burden. Hence, due to the short runtime of the proposed protocol even for short time intervals of data transmission, it may be considered as a super-lightweight authentication scheme to be deployed in future *NAN* communication of the smart grid.

The studied protocols in this paper endure of single point of failure which is due to their centralized infrastructure. As the world is changing every day, trusting one entity will be less and less judicious. Hence, many applications are inclined to use blockchain technology to eliminate the trusted third

party and distribute the role of that entity to the participating nodes of the network. This may result in the total elimination of the control center or even the *NG*s. Thus, the existing hierarchical layer may go experience a thorough adjustment in the future. On the other hand, because of the elimination of the trusted party, now the non-trusting involved nodes must act as the server and compute the necessary functions on each other's sensitive data, hence, the secrecy of these data is crucial. In other words, a multi-party computation (MPC) protocol can be used to allow the nodes to perform any function they need on their inputs without revealing them. However, not many MPC protocols have been introduced to be used in resource constraint networks. Thus, introducing a lightweight scalable blockchain-based MPC protocol suitable for rescores constraint networks like smart grid would be an interesting and challenging topic for the future work.

APPENDIX

In this section a brief description of Boyd and Mao logic will be provided. The goal of this logic is to prove that the secret values of the protocol are indeed secret and will not be exposed to unauthorized users. At first the meaning of the used notations are given.

$A \mid\equiv B$: A believes B (B is true and acts accordingly).

$A \overset{k}{\leftrightarrow} B$: k is a good shared key for A and B.

$A \overset{k}{\mid\sim} B$ is encrypted by A using the key k.

$A \overset{k}{\triangleleft} B$: A obtains B by using k as the deciphering key

$A \triangleleft B$: A sees the message B.

$\#A$: A is new and fresh and has not been used before.

$A \triangleleft \| B$: A cannot see the plain message B.

$sup(A)$: A is the trusted party.

Now we provide the important rules of this logic.

Authentication Rule: $\frac{A\mid\equiv A \overset{k}{\leftrightarrow} B \wedge A \overset{k}{\triangleleft} C}{A\mid\equiv B \overset{k}{\mid\sim} C}$. This rule implies that if k is the shared key between A and B and A decrypted C by using k then A believes that B has sent the message C.

Confidentiality Rule: $\frac{A\mid\equiv A \overset{k}{\longleftrightarrow} B \wedge A\mid\equiv S^c \triangleleft \| C \wedge A \overset{k}{\mid\sim} C}{A\mid\equiv (S\cup\{B\})^c \triangleleft \| C}$. if k is a shared key between A and B and the key has not been shared to anyone else then if A encrypt C using the key k this rule indicates that A believes that no one except the trusted party and B can obtain the message C.

Super principle Rule: $\frac{A\mid\equiv B\mid\equiv C \wedge A\mid\equiv sup(B)}{A\mid\equiv C}$. If A believes B as a trusted party and also believes what the trusted party believes, then this rule concludes that A believes what the trusted party believes.

The Fresh Rule: $\frac{A\mid\equiv \#(C) \wedge A \triangleleft D \,\mathfrak{R}\, C}{A\mid\equiv \#(D)}$, where $\mathfrak{R}$ is the concatenation notation. This rule implies that if A believes that the message C is fresh and then it sees the message C concatenated with another message D then A believes that the message D is fresh too.

The Good-key Rule 1: $\frac{A\mid\equiv \{A,B\}^c \triangleleft \| k \wedge A\mid\equiv \#(k)}{A\mid\equiv A \overset{k}{\longleftrightarrow} B}$. If A believes that no one else except himself and B knows the key and also believes that the key k is fresh, then A believes that k is a good shared key between him and B.

The Good-key Rule 2: $\frac{A\mid\equiv \{A,B,C\}^c \triangleleft \| k \wedge A\mid\equiv sup(C) \wedge A\mid\equiv \#(k)}{A\mid\equiv A \overset{k}{\longleftrightarrow} B}$. If A believes that only A, B and C knows the key k, and the key is fresh and C is a trusted party, then A concludes that k is a good shared key.

Intuitive Rule: $\frac{A \overset{k}{\triangleleft} B}{A \triangleleft B}$. If A can decrypt the message B by using k, it can see the message.

Derived Rule: $\frac{A\mid\equiv B\mid\equiv A \overset{k}{\longleftrightarrow} B \wedge A\mid\equiv B\mid\equiv S^c \triangleleft \| C \wedge A\mid\equiv B \overset{k}{\mid\sim} C}{A\mid\equiv B\mid\equiv (S\cup\{A\})^c \triangleleft \| C}$. This rule is derived from both Confidentiality Rule and a belief axiom stating $A \mid\equiv (X \wedge Y)$ if and only if $A \mid\equiv X \wedge A \mid\equiv Y$.

ACKNOWLEDGMENT

The authors would like to acknowledge the National Iranian Gas Company for its unwavering supports.

REFERENCES

[1] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016.
[2] M. H. Ameri, M. Delavar, and J. Mohajeri, "Provably secure and efficient PUF-based broadcast authentication schemes for smart grid applications," *Int. J. Commun. Syst.*, vol. 32, no. 8, p. e3935, May 2019.
[3] R. Amin, S. Kunal, A. Saha, D. Das, and A. Alamri, "CFSec: Password based secure communication protocol in cloud-fog environment," *J. Parallel Distrib. Comput.*, vol. 140, pp. 52–62, Jun. 2020.
[4] S. M. Sedaghat, M. H. Ameri, M. Delavar, J. Mohajeri, and M. R. Aref, "An efficient and secure attribute-based signcryption scheme for smart grid applications," Scientia Iranica, Cryptol. ePrint Arch., Tech. Rep. 2018/263, 2018. [Online]. Available: https://eprint.iacr.org/2018/263
[5] S. Aghapour, M. Kaveh, D. Martín, and M. R. Mosavi, "An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications," *IEEE Access*, vol. 8, pp. 125477–125487, 2020.
[6] S. Rajamanickam, S. Vollala, R. Amin, and N. Ramasubramanian, "Insider attack protection: Lightweight password-based authentication techniques using ECC," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1972–1983, Jun. 2020.
[7] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[8] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.
[9] 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," *Comput. Electr. Eng.*, vol. 52, pp. 114–124, May 2016.
[10] S. Uludag, K.-S. Lui, W. Ren, and K. Nahrstedt, "Secure and scalable data collection with time minimization in the smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 43–54, Jan. 2016.
[11] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.
[12] Y. Liu, C. Cheng, T. Gu, T. Jiang, and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors J.*, vol. 16, no. 3, pp. 836–842, Feb. 2016.
[13] D. Abbasinezhad-Mood and M. Nikooghadam, "An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an ARM cortex-M microcontroller," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6194–6205, Nov. 2018.
[14] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.
[15] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3548–3557, May 2020.

[16] V. Sureshkumar, S. Anandhi, R. Amin, N. Selvarajan, and R. Madhumathi, "Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication," *IEEE Syst. J.*, early access, Dec. 10, 2020, doi: 10.1109/JSYST.2020.3039402.
[17] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.
[18] M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, Jun. 2017.
[19] S. Rohjans, M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, and T. Weidelt, "Survey of smart grid standardization studies and recommendations," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 583–588.
[20] S. Erlinghagen, B. Lichtensteiger, and J. Markard, "Smart meter communication standards in Europe—A comparison," *Renew. Sustain. Energy Rev.*, vol. 43, pp. 1249–1262, Mar. 2015.
[21] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 425–436, Feb. 2016.
[22] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2831–2848, 3rd Quart., 2019.
[23] W. Mao and C. Boyd, "Towards formal analysis of security protocols," in *Proc. 4th Comput. Secur. Found. Workshop*, 1993, pp. 147–158.
[24] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[25] *ArduinoLibs: Cryptographic Library*. Accessed: 2019. [Online]. Available: http://rweather.github.io/arduinolibs/crypto.html
[26] *Atmel's Family of Smart Power Meters*. Accessed: 2019. [Online]. Available: https://www.microchip.com/design-centers/smart-energy-products/metering

SAEED AGHAPOUR received the B.Sc. degree in electrical engineering from the Babol Noshirvani University of Technology, Iran, in 2014, and the M.Sc. degree in electrical engineering major of communication cryptology from the Sharif University of Technology (SUT), Iran, in 2016. His research interests include advance cryptography, provable security, security analysis of cryptographic protocols, smart grid, and the IoT security.

MASOUD KAVEH received the B.Sc. degree from the Babol Noshirvani University of Technology, Iran, in 2014, and the M.Sc. degree from the Marine Sciences University of Nowshahr established in collaboration with the Iran University of Science and Technology (IUST), Iran, in 2016, all in electrical engineering. He is currently pursuing the Ph.D. degree with IUST. His research interests include physical unclonable functions (PUFs), cryptographic protocols, ASIC and FPGA design, and machine learning.

MOHAMMAD REZA MOSAVI received the B.S., M.S., and Ph.D. degrees in electronic engineering from the Iran University of Science and Technology (IUST), Tehran, Iran, in 1997, 1998, and 2004, respectively. He is currently a Faculty Member (Full Professor) of the Department of Electrical Engineering, IUST. He has authored more than 400 scientific publications in journals and international conferences, in addition to 11 academic books. His research interest includes circuits and systems design. He is also the Editor-in-Chief of *Iranian Journal of Marine Technology* and an Editorial Board Member of *Iranian Journal of Electrical and Electronic Engineering*.

DIEGO MARTÍN received the B.Sc. degree in computer engineering and the M.Sc. degree in computer science from the Department of Informatics, Carlos III University of Madrid, Spain, and the Ph.D. degree from the Department of Informatics, Carlos III University of Madrid, in 2012. He is currently a Lecturer with the Department of Telematics, Technical University of Madrid (UPM). His main research subjects within the GISAI groups at UPM are the Internet of Things (IoT), cyber physical systems, physical unclonable functions (PUFs), blockchain, knowledge management, information retrieval, and research methods.