IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received June 8, 2020, accepted June 29, 2020, date of publication July 7, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007623

An Ultra-Lightweight and Provably Secure Broadcast Authentication Protocol for Smart Grid Communications

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

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

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

ABSTRACT The information and communication technology (ICT) can bring attractive features to the traditional power grid such as energy conserving, reliability, efficiency, transparency, and cost reducing. All of these features can be accomplished with a concept called smart grid. However, the use of ICT introduces new challenges in security issue. There are many researches in recent years which have studied security as the most important challenge of the smart grid. Based on these researches, two important issues for the smart grid security protocols must be considered. In the first issue, the important security requirement such as confidentiality, authentication, integrity, etc. needs to be fulfilled. However, the cryptographic algorithms impose significant level of storage, communication, and computational costs to the system while, the smart meters are resource-constrained devices. Therefore, lightweight design of the security schemes is considered as another important issue. To that end, this paper proposes a novel provably secure broadcast authentication scheme based on one-way hash function, which not only can resist to the possible existing attacks but also dramatically reduces the storage and computational costs.

INDEX TERMS Broadcast communication, lightweight authentication, provable security, smart grid.

I. INTRODUCTION

Daily growing of the information and communication technology (ICT) has improved the efficiency and reliability of the traditional power grid, and led to introducing to an important concept named smart grid [1]–[3]. ICT enhances the one-way electrical flow by providing two-way communication in the smart grid so that the utility service provider can continuously receive reports from the smart meters (*SM*s) through the neighborhood gateways (*NG*s) and send control messages to them [4].

Although using of ICT has its own advantages, it brings up some serious challenges in the case of security [5]–[10]. For example, by capturing and eavesdropping the exchanged messages between the *SM*s and *NG*, an adversary can access to the private information of the consumers, e.g. knows their presence or absence hours at home by learning their daily electricity consumption [11]–[14]. Furthermore, the adversary can replay the old packets, alter the electricity reports of the *SM*s, or inject fake messages to the *NG*s and consequently tricks the utility service provider to make wrong decisions [15]–[18].

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

A. SYSTEM MODEL

Fig. 1, shows the hierarchical model of both power system layer and communication layer of the smart grid. In the first level of power system layer, the power generation unit generates the needed energy for consumers. The power transmission network carries the power from the bulk generation facilities to the power distribution systems. The power distribution system finally delivers the electricity from the transmission system to consumers. The smart grid communication layer uses ICT to optimize the energy generation, transmission and distribution. The first level of the communication layer is home area network (*HAN*) where *SM* collects the electricity information from some smart appliances. At the second level, *NG* receives the electricity reports from a certain numbers of *SM*s (a few hundreds) and send

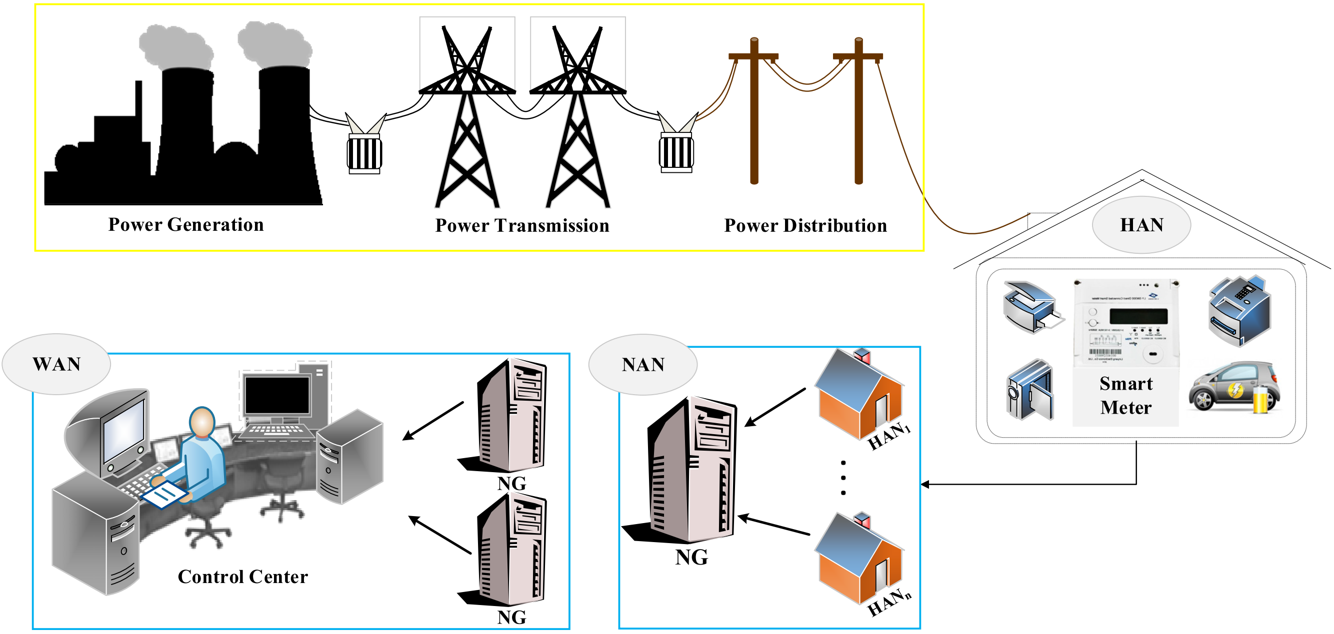


FIGURE 1. Smart grid architecture: The blue line shows the communication layer and the yellow line shows the power system layer.

the control commands back to them. This level is named a neighborhood area network (*NAN*). At the top level, in a wide area network (*WAN*), the control center collects all the *SM*s' energy consumption reports from *NG*s and makes the final decisions. In the general architecture of smart grid, *WAN* corresponds to power generation and transmission systems, *NAN* corresponds to power distribution system, and *HAN* includes communications related to the consumers [1]–[4]. This paper is going to propose a secure broadcast two-way communication protocol for the *NAN* communication system where *NG* with a high computational capacity and large database storage capacity tries to collect electricity reports from constrained resource *SM*s.

B. RELATED WORKS

Through years, many schemes have been proposed to address the security as the most important issue in the smart grid [5]–[21]. Li *et al.* [19] proposed an authentication scheme based on Merkle hash tree and Advanced Encryption Standard (AES) for establishing secure communication between the *SM*s and *NG* in 2014. The authors in [19] showed that their proposed protocol is secure against the replay, message injection, message analysis, and message modification attack. In addition, their performance evaluation showed that their proposed scheme is efficient in terms of communication overhead and computational cost.

In 2016, Liu *et al.* [20] proposed an authenticated communication scheme for the smart grid based on the Lagrange polynomial formula. The authors in [20] showed that their scheme could resist against the mentioned attacks, while outperforming Li *et al.* [19] in terms of storage burden, communication overhead, and computational cost.

One of the most important drawbacks of the mentioned methods is lack of two-way communication between *NG* and *SM*, and even if considered, it implies significant costs on the system for sending messages from *NG* to *SM*s which is in contradiction of low capability of resources constrained devices.

Recently, Abbasinezhad-Mood and Nikooghadam [21] proposed an ultra-lightweight and secure communication scheme in 2018 based on logical XOR, pseudo-random number generator, and one-way hash function. The authors in [21] showed that their scheme possess higher security level and can resist against more attacks comparing to proposed schemes in [19] and [20]. Furthermore, they showed that their protocol significantly improves the storage burden, communication overhead, and computational cost in comparison with the state-of-the-art.

However, in most smart grid applications, *NG* needs to send identical control messages to the all or specific group of *SM*s. Hence, by utilization of the broadcast communication, the need of sending multiple unicast messages will be eliminated, which significantly reduces the expenses in smart grid [22]–[25]. Despite the fact that using the broadcast authentication adds attractive features to smart grid, the concept of security in this type of communication differs from the unicast ones [26]–[30]. For that, some broadcast authentication schemes have been proposed in recent years to address this issue [31]–[33].

Li and Cao [31] proposed a multicast authentication scheme based on one-time signature. They specifically proposed tunable signing and verification (TSV) and light signing heavy verification (LSHV) for smart grid applications. They showed that in comparison to the previous works, their proposed one-time signature based scheme could significantly reduce the storage burden, communication overhead, and computational cost while providing the same security level as those schemes possess.

In 2017, Delavar *et al.* [32] proposed a broadcast authentication scheme based on Physical Unclonable Function (PUF) named PUF-BA. They proposed their scheme with assumption that SMs are computationally resources constraints and the expense of communication grows as the number of connected SMs increases. In addition, they assumed that SMs are located in an unprotected environment which can be physically threatened by adversaries. Although their scheme was proposed for networks with resources constrained devices, yet it required high computational power from SMs.

To overcome the high computational overhead of [32], quite recently in 2019, Ameri *et al.* [33] proposed a provably secure broadcast authentication scheme for smart grid based on PUF. They used the advantage of Bose–Chaudhuri–Hocquenghem (BCH) coding algorithm for error correcting to make the PUF responses reliable. Although they proved that their protocol provides a high level of security and reduces the computational cost dramatically compared to [32], the computational cost and storage burden were still significant based on SMs' capabilities.

C. PAPER CONTRIBUTION

This paper aims at proposing a new security protocol for two-way communication between SMs and NG in the smart grid only based on lightweight cryptographic operations, i.e. one-way hash function and XOR operand. We show that, not only does the proposed protocol add some important features to the communication system such as mutual authentication, two-way communication, one-time pad cryptographic key, and confidentiality of the SMs' data but also it provides significant level of efficiency in terms of storage burden, communication overhead, and computational cost. Therefore, the proposed scheme can be considered as a practical security protocol for near future of the smart grid communications. The contributions of this paper can be summarized as follows:

- Being secure against the possible attacks in the smart grid communication system environment, i.e. impersonation, message modification, message analysis, replay, and compromised malicious SM attack.
- Efficiently ensuring mutual authentication and two-way communication between the SMs and NG.
- Providing a provable security analysis for our protocol.
- Deploying a One-time Pad (OTP) system that uses each communication key once and a fresh key is used for each time interval to increase the protocol resistance against the brute-force attack.
- Consuming the lowest overhead among the related work in terms of storage, communication, and computational costs, which will make it suitable to use in the networks with very resources constrained SM devices.

TABLE 1. Notations and their meanings.

Symbol	Description
$H(.)$	The one-way hash function
ID^j	Identifier of SM_j
D_i^j	ith usage report of SM_j
r_i	ith generated random numbers by NG
TS^{SM_j}	Timestamp of SM_j
TS^{NG}	Timestamp of NG
TS_i	Beginning time of time interval i
SM_j	jth smart meter
NG	Neighborhood gateway
K_i	The ith broadcast key
V_i	ith message verifier of NG
m_i	ith broadcasted control message
σ	Key disclosure delay
E_i^j	ith encrypted message of SM_j
Z_i^j	ith unicast key of SM_j
V'^j_i	ith message verifier of SM_j
λ	Security parameter
PP	Public parameters
l	Number of all smart meters
i	The ith communication
$\oplus$	The XOR operand
N	Length of hash chain
$negl(\lambda)$	A negligible amount
m_i^*	ith forged broadcast message
D_i^{j*}	ith forged data report of SM_j
$\|T\|$	Length size of the parameter T
t	Number of compromised smart meters
T^*	Forged T parameter
BF	Bloom filter
HD	PUF's helper data
(C,R)	PUF's challenge and response

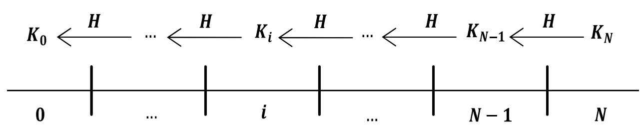


FIGURE 2. The hash key chain.

The remainder of this paper is organized as follows. The proposed scheme is presented in section II thoroughly. Security analysis and formal security proof are provided in section III and section IV, respectively. Section V evaluates the performance of the proposed scheme in comparison with the state-of-the-art, and finally, section VI concludes of this paper.

II. PROPOSED SCHEME

In this section, we introduce the proposed scheme with details. The proposed scheme is consisted of two stages: an offline installation stage and an online communication stage. Table 1 shows the used notations and their corresponding meanings.

A. OFFLINE INSTALLATION STAGE

In this stage, first NG creates a hash key chain by choosing a random value K_N and using a one-way hash function like H to create the broadcast keys $K_0, \ldots, K_{N-1}$, by computing each key as $K_i = H(K_{i+1}) = H^{N-i}(K_N)$. Fig. 2 depicts the process of the creation of the hash chain. It is worth noting, that by having the key K_i all of the backward keys $K_0, \ldots, K_{i-1}$ can be computed easily by executing a number of hash functions. However, because of using a one-way collision resistance hash function, finding the next key K_{i+1} by having K_i is computationally hard for polynomial time computers.

After completing the key chain, NG broadcasts the initial key K_0 through the network. Furthermore, after each Sm_j registered itself to NG, a secret random parameter Z_0^j will be allocated to it by NG through a secure link. Then, each SM stores its secret key Z_0^j alongside the initial broadcast key K_0 in its memory and NG stores K_N and Z_0^j for $j = 1, \ldots, l$, which l is the number of smart meters. Note that, NG can store all of the broadcast keys $K_0, \ldots, K_{N-1}$ in its memory, to decrease its computational overhead at the cost of an increase in its storage burden.

B. ONLINE COMMUNICATION STAGE

As mentioned before, the proposed protocol presents a two-way communication meaning that in each communication interval, NG broadcasts its message through the network of l smart meters then, after receiving the message each smart meters sends its data report to NG unicastly. Hence, we divide the protocol to two parts naming the broadcast part and the unicast part. Fig. 3 depicts the online communication stage of the proposed protocol.

1) COMMUNICATION FROM NG TO ALL OF THE SMs (BROADCAST PART)

In this part, for each run of the protocol NG performs the following steps:

- Computes the i^{th} broadcast key $K_i = H^{N-i}(K_N)$.
- Generates a random number r_i.
- Creates the message verifier $V_i = H(m_i, TS^{NG}, K_i, r_i)$ to provide message authenticity and freshness.
- Broadcasts the packet $\{m_i, V_i, TS^{NG}\}$ through the network.
- After a specific delay time of σ which depends to the network environment, broadcasts the corresponding key K_i and the random number r_i.

As mentioned before, NG only broadcasts its message at beginning of the certain time intervals TS_i. It is worth noting that at the beginning of each time interval, the smart meters wait at most σ seconds to receive the packet and any packets, which are received after that time, will be discarded by SMs immediately. In other words, after the first broadcasted packet $\{m_i, V_i, TS^{NG}\}$ is received, each SM_j checks if the equation $TS^{SM_i} - TS_i \leq \sigma$ holds or not. Because, the scenario where the mentioned equation does not hold, results to the occasion that the received packet could be a forged one computed by adversaries, because an adversary can block the transmission and wait for the disclosure delay σ to receive the corresponding key and then by using it, creates its own forged authentic packets. As a result, to prevent this attack all of the packets with the received time stamp of more than $TS_i + \sigma$ will be discarded by SMs.

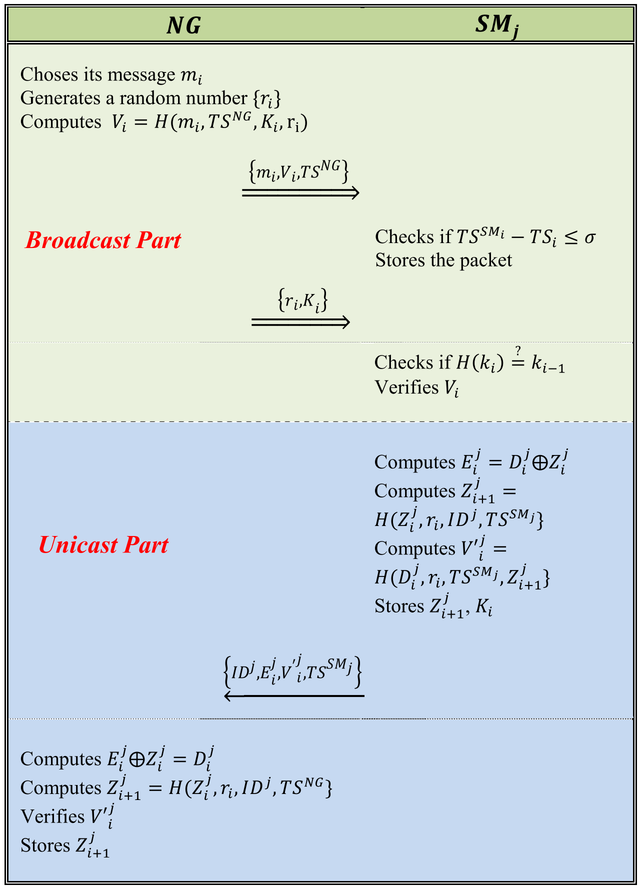


FIGURE 3. The online communication stage of the proposed protocol.

Now, only if the equation $TS^{SM_i} - TS_i \leq \sigma$ holds, each of the smart meters store the packet $\{m_i, V_i, TS^{NG}\}$ in their memory and waits for the disclosure of K_i and r_i. Then, after the packet $\{r_i, K_i\}$ is received each of the smart meters act as follows:

- Verify the validity of the key by checking if the equation $H(K_i) = K_{i-1}$ holds or not.
- Verify V_i to make sure the message is fresh and has not been altered by adversaries.
- Accept the message should the two verification processes succeed. Otherwise discards the packet.
- Update the previous broadcast key K_{i-1} to K_i in their memory. At this point, the broadcast stage is completed.

2) COMMUNICATION FROM EACH SM_j TO THE NG (UNICAST PART)

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

- Compute $E_i^j = D_i^j \oplus Z_i^j$ as their encrypted message.
- Compute $Z_{i+1}^j = H(Z_i^j, r_i, ID^j, TS^{SM_j})$ as their next unicast key.
- Compute $V'^j_i = H(D_i^j, r_i^j, TS^{SM_j}, Z_{i+1}^j)$ as their message verifier.
- Send the packet $\left\{ID^j, E_i^j, V_i'^j, TS^{SM_j}\right\}$ to NG.
- Store Z_{i+1}^j in their memory.

The need for using a unique secret key for each of the SM_j is that the smart meters must not be able to have access to each other's data reports and their reports have to be encrypted by a secret key which is known only by each SM_j and the NG.

Upon receiving the packets $\left\{ID^j, E_i^j, V_i'^j, TS^{SM_j}\right\}$ from smart meters, for $j = 1, \ldots, lNG$ acts as follow:

- Decrypts E_i^j by computing $E_i^j \oplus Z_i^j = D_i^j$ to obtain the data report D_i^j.
- Computes the unicast key $Z_{i+1}^j = H(Z_i^j, r_i, ID^j, TS^{SM_j})$.
- Verifies V'^j_i for checking the authenticity of the received packets.
- Stores Z_{i+1}^j in its memory.

Note that, the use of Z_{i+1}^j in the verifier V'^j_i helps SM_j to make sure that NG has computed the next unicast key successfully and is able to decrypt the next encrypted message. However, if NG is unable to verify $V_i'^j$, it can request SM_j to resend its packet. Furthermore, it is important to mention that the length size of parameters ID_j and TS are considered 16 bit and r_i and m_i are considered to be of 128 bit length size. Also E_i^j and D_i^j and the hashed values V_i, K_i, Z_i^j, and V'^j_i are all considered to have 256-bit length.

III. SECURITY ANALYSIS

In this section after introducing the threat model, the security of the proposed scheme against the possible threats are studied.

A. THREAT MODEL

In this paper, it is considered that a Probabilistic Polynomial Time (PPT) adversary can eavesdrop and has access to communicated packets. As a result, he/she can alter or inject its own messages to the communication to perform different possible attacks in the NAN communication system such as impersonation attack, message modification attack, message analysis attack, replay attack, and compromised malicious SM attack [19]. In what follows explaining each of these attacks with details, we investigate the resistance of the proposed protocol against them.

B. IMPERSONATION AND MESSAGE MODIFICATION ATTACK

In this kind of attacks, the adversaries' strategy is to act as a middle-man and after receiving the communication messages alter them in such a way to pass the verification process in the other end. The attack can be performed in both sides of the communication. In other words, the adversary can impersonate either one the smart meters or NG. However, we see that the existence of the message verifier, which is created by a collision free one-way hash function, prevents these kinds of attacks.

As for the first scenario, we consider the adversary is attacking the scheme by impersonating the NG. In this scenario by having the broadcasted packet $\{m_i, V_i, TS^{NG}\}$ the adversary's goal is to create the verifier for its own message m_i^* as $V^* = H(m_i^*, TS^{NG}, K_i, r_i)$. However, as K_i and r_i are not disclosed yet and also because the key is created from a hash chain by the NG in the setup stage and cannot be computed by anyone else, the probability of success of any adversary with polynomial time computational power in creating the corresponding verifier for their messages is negligible.

As for the second scenario, adversaries attack the protocol at SM's side by impersonating SM_j. By eavesdropping the adversaries have access to the transmission packets and can obtain $E_i^j = D_i^j \oplus Z_i^j$ and $V'^j_i = H(D_i^j, r_i, TS^{SM_j}, Z_{i+1}^j)$. Now, their goal is to change the message D_i^j to D_i^{j*} and create $E_i^{j*} = D_i^{j*} \oplus Z_i^j$ and the corresponding verifier $V'^{j*}_i = H(D_i^{j*}, r_i, TS^{SM_j}, Z_{i+1}^j)$. Nevertheless, as the unicast key Z_i^j is secret and shared only between each SM_j and NG separately, the adversary has no knowledge of it. Hence, they are not able to compute Z_{i+1}^j to compute the verifier V'^{j*}_i. As a result, the probability of adversaries' success for forging the valid corresponding verifier for their desired messages is negligible.

C. MESSAGE ANALYSIS ATTACK

In this attack, after eavesdropping on the communication link from SM_j to NG, the adversaries try to decrypt the packet and find the data report. In other words, by having $E_i^j = D_i^j \oplus Z_i^j$ the adversary tries to find the data report D_i^j. However, as the unicast key Z_i^j is shared between each SM_j and the NG secretly, and no one else knows it and moreover, because this key changes after one usage in each communication interval, the security of the proposed scheme against this attack reduces to the security of the one-time pad crypto system. Thus, the attack is not practical for PPT adversaries.

D. REPLAY ATTACK

In replay attacks, the adversaries store the once sent valid communication packets and resend them later with the hope to pass the verification process in the other end. Because of the two-way nature of the proposed scheme, the attack can be performed in both side of the protocol.

In attacking the broadcast communication from NG to smart meters, the adversaries broadcast the once sent packet $\left\{m_i, V_i, TS^{NG}\right\}$ which had been sent in time interval i in another time interval like b. Then, after the disclosure delay is passed, broadcast the corresponding key and the random number $\{K_i, r_i\}$ through the network. However, as the first thing smart meters do is to check the validity of the corresponding key the packet will be discarded immediately after the key is disclosed because, the probability that the equation

$H(K_i) = K_{b-1}$ holds is negligible and that is because the one-way hash function is considered to be collision free.

For the second part of the protocol, the adversaries send the packet $\left\{ID^j, E_i^j, V_i^{\prime j}, TS^{SM_j}\right\}$ which had been sent in time interval i to NG in another time interval b. However, upon receiving the packet, because of the existence of the time stamp in message verifier $V_i^{\prime j} = H(D_i^j, r_i^j, TS^{SM_j}, Z_{i+1}^j)$, the old verifier is not valid anymore and NG discards the packet immediately. Therefore, the proposed scheme is secure against the replay attack.

E. COMPROMISED MALICIOUS SM ATTACK

In this attack, we investigate the security of the proposed scheme against the situation where t number of smart meters become malicious and compromise to disrupt the protocol. The disruption could be either trying to forge a broadcast message or trying to read data reports of other not-compromised smart meters. The difference between investigating of this attack and the injection attack is that in this attack the unicast keys of t smart meters $\left\{Z_i^j\right\}_{1\leq j\leq t}$ are also known. Similarly, based on which part of the proposed protocol is being attacked, we divide it to two scenarios.

In the first case, the compromised smart meters want to broadcast a valid authenticated packet through the network. In other words, by having $\left\{Z_i^j\right\}_{1\leq j\leq t}$ and the broadcasted packet $\left\{m_i, V_i, TS^{NG}\right\}$, they try to forge their verifier $V^* = H(m_i^*, TS^{NG}, K_i, r_i)$ for their message m_i^*. However, as this part of the protocol is independent from the unicast part, using $\left\{Z_i^j\right\}_{1\leq j\leq t}$ is futile and based on the former analyzes the attack is not feasible. In the second scenario, the compromised smart meters try to use their unicast keys to decrypt other SMs' encrypted transmission data reports. We assume t compromised SMs are $\left\{SM_j\right\}_{1\leq j\leq t}$ hence; their corresponding unicast keys $\left\{Z_i^j\right\}_{1\leq j\leq t}$ are exposed. Now, the goal is to decrypt an encrypted message $E_i^k = D_i^k \oplus Z_i^k$ where $k > t$ and $Z_i^k = H(Z_{i-1}^k, r_{i-1}, ID^k, TS^{SM_k})$. However, as the unicast key Z_{i-1}^k is not exposed and also this key is independent from $\left\{Z_i^j\right\}_{1\leq j\leq t}$, the probability of success in this attack is negligible for PPT adversaries.

IV. FORMAL SECURITY PROOF

In this section, we aim to prove the security of broadcast part of the proposed scheme against chosen message attack. As mentioned before, we assumed that the data communication in the offline installation stage is performed in a secure channel and then cannot be eavesdropped by adversaries. However, the online communication stage is performed in an insecure environment thus; the communicated data in this stage can be eavesdropped and altered by adversaries. Furthermore, we assume that NG is physically secure and cannot be compromised by adversaries and only smart meters are vulnerable to adversaries. Besides that, the function H is considered as a one-way collision free hash function that means the probability of finding $x \neq y$ where $H(x) = H(y)$ is computationally hard for adversaries with polynomial computational power.

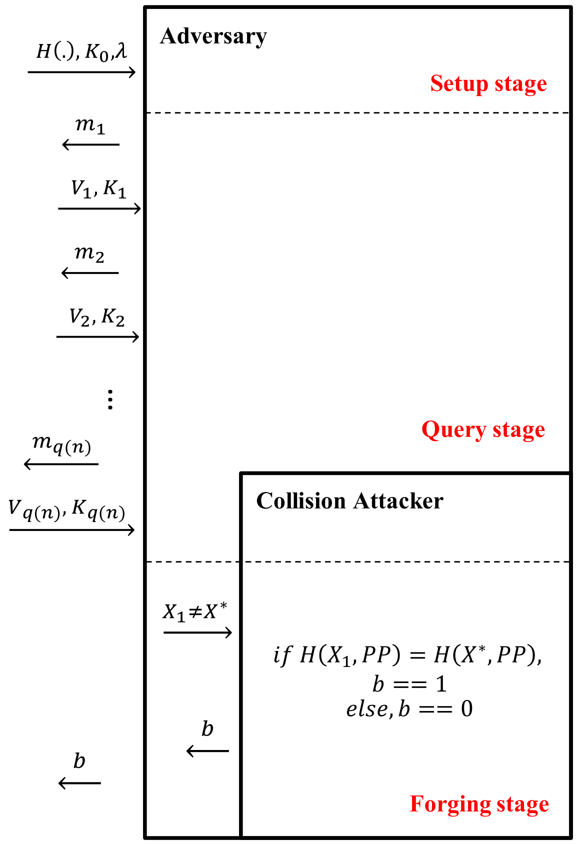


FIGURE 4. Adversary model in the CMA game.

In what comes next, we prove the security of the scheme against chosen message attack. The overall goal of the adversaries is to use the released information in former time intervals to forge a new valid and authenticated broadcast message for the next time interval. Chosen message attack (CMA) is defined through a game, which is depicted in Fig. 4. In this attack, the adversary adaptively choses arbitrary messages and receives the corresponding response for the selected message. After that, the adversary tries to forge a new broadcast packet for its chosen message to pass the verification process in smart meters' end. The game is performed in three stages: Setup stage, query stage and forging stage.

In the setup stage, by selecting the security parameter λ and the hash function $H(\cdot)$, the challenger computes the broadcasts keys by applying the hash key chain by choosing a random parameter K_N and sends the tuple $\{K_0, \lambda, H(\cdot)\}$ to the adversary A.

In the query stage, the adversary can request the challenger to get the responses to a polynomial number of his arbitrary messages. In other words, for

$i = 1, \ldots, q(n)$ the adversary can adaptively choses different or same messages like $m_1, \ldots, m_{q(n)}$ and sends them to the challenger. The challenger by running the protocol, gives adversary the corresponding responses $\{V_1, K_1\}, \ldots, \{V_i, K_i\}, \ldots, \{V_{q(n)}, K_{q(n)}\}$ where $V_i = H(m_i, TS^{NG}, K_i, r_i)$ and $H(K_{i+1}) = K_i$. Note that, for simplicity and without loss of generality, r_i and TS which are public are not brought in the responses.

In the forging stage, in order for passing the verification process, the adversary's goal is to output a tuple $(m^*, V^*, K_{q(n)+1}, r_{q(n)+1})$ where $V^* = H(m^*, TS, K_{q(n)+1}, r_{q(n)+1})$. Hence, the adversary's goal reduces to computing $K_{q(n)+1}$ such that $H\left(K_{q(n)+1}\right) = K_{q(n)}$. For simplicity, we denote $K_{q(n)+1} = X_1$ and $K_{q(n)} = X_0$. Hence, the probability of adversary's success is equal to be able to guess a parameter X^* to satisfy the following equation:

$$\Pr\left\{A^{Wins}\right\} = \Pr\{X^* | H\left(X^*\right) = X_0, 1 \leftarrow Vrfy(PP, X^*)\}$$

where $PP = \left\{\{K_i\}_{0 \le i \le q(n)}, \{r_i\}_{0 \le i \le q(n)}, TS\right\}$ is the public and disclosed parameters. Thus, we have:

$$\begin{aligned} &Pr\left\{H\left(X^*\right) = X_0, 1 := Vrfy\left(PP, X^*\right)\right\} \\ &\quad = Pr\{H(X^*) = X_0, 1 := Vrfy\left(PP, X^*\right) | X_1 \\ &\qquad \neq X^*\} Pr\left\{X_1 \neq X^*\right\} \\ &\qquad + Pr\{H(X^*) = X_0, 1 := Vrfy\left(PP, X^*\right) | X_1 \\ &\qquad = X^*\} Pr\left\{X_1 = X^*\right\} \end{aligned}$$

By having the security parameter of λ, we have $\Pr\{X_1 = X^*\} = \frac{1}{2^\lambda} = negl(\lambda)$ and $\Pr\{X_1 = X^*\} = 1 - negl(\lambda)$. Hence, the equation will simplify to:

$$\begin{aligned} &Pr\left\{H\left(X^*\right) = X_0, 1 := Vrfy\left(PP, X^*\right)\right\} \\ &\qquad = Pr\{H(X^*) = X_0, 1 := X_1 \neq X^*\} + negl(\lambda) \end{aligned}$$

Furthermore, as mentioned before the first step in verification process is to check the authenticity of the key and then check the message integrity by running the $Vrfy(\cdot)$ algorithm. Note that, $Vrfy(\cdot)$ outputs 1 should the equation $H\left(X^*\right) = X_0$ holds otherwise outputs 0. As a result the probability of A's success reduces to:

$$\begin{aligned} Pr\left\{A^{Wins}\right\} &= Pr\{H(X^*) = X_0, 1 := Vrfy(PP, X^*) | X_1 \\ &\quad \neq X^*\} + negl(\lambda) \\ &= Pr\{H\left(X^*\right) = X_0, X_1 \neq X^*\} + negl(\lambda) \end{aligned}$$

where $Pr\{H\left(X^*\right) = X_0, X_1 \neq X^*\}$ means finding a parameter $X_1 \neq X^*$ that $H\left(X^*\right) = X_0 = H(X_1)$ which is an expression of finding a collision in the hash function.

$$\Pr\left\{A^{Wins}\right\} = \Pr\left\{A^{Coll}\right\} + negl(\lambda)$$

As in this paper, we considered that the hash functions are collision free against the polynomial time computers meaning $\Pr\left\{A^{Coll}\right\}$ is negligible Hence:

$$\Pr\left\{A^{Wins}\right\} \le negl(\lambda)$$

V. COMPARATIVE PERFORMANCE EVALUATION

In this section, the performance of the proposed scheme is evaluated and compared with the proposed schemes in [31]–[33] in terms of storage burden, communication overhead, and computational cost. For this purpose, a SHA-256 is used to execute the cryptographic hash function. For comparing the performance of the proposed protocol in this paper with the state of the art comprehensively, the time interval of each data transmission is considered fifteen minutes (ninety six electricity data transmission per day). Then, to have a real-time perspective for the future communication of the smart grid, we evaluate the performance of the all schemes for various time intervals from one minute to fifteen minutes.

Furthermore, as the proposed schemes in [31]–[33] use different cryptographic primitives, to have a meaningful and comprehensive comparison we assume a logical, balanced and length for those primitives. Hence, 530, 256, and 128 bits are assumed for PUF challenges, output of SHA-256 hash functions, and PUF responses, respectively where for simplicity we notated them by C, H, and R. In addition, the size of each time interval i is considered 16 bit. The output length of bloom filter which is notated by BF is considered to be of 144 bit and for error correcting of the PUF, 2052 bit is used as a helper data being notated by HD. Needless to say, because of non-existence of idealized PUF, helper data is used to help the smart meters to be able to recover the same PUF responses. Moreover, the proposed scheme in [32] used three parameters computed as $X = g^\sigma, y = g^r, W = r + cz_j\sigma$ which we considered to have 2048-bit, 2048-bit, and 768-bit length, respectively. In addition, in proposed scheme in [31], the authors considered that the private key is consisted of t parameters where each of them has l bit length. With respect to their reference paper and for having the same security level as other mentioned schemes possess, we consider t and l to be of 128 and 256 bit length, respectively. The detailed performance evaluation analysis of the proposed scheme in this paper compared to those proposed in [31]–[33] is described in the rest of this section.

A. STORAGE BURDEN

It is assumed that NG is a server that is equipped with a large database with very high storage capacity. Therefore, we only calculate the storage burden for the SM side. However, our scheme has the lowest storage burden for NG side compared with the other mentioned schemes.

As mentioned in section II, in the proposed scheme, each SM only needs to store Z^j_{i+1} and K_i in its memory for future key generation and data transmission. Since as we use SHA-256 for executing a one-way hash function, the total storage cost of our scheme is equal to $2 \times H = 64B$. Table 2 demonstrates the number of required stored parameters in each SM's memory for our scheme and also proposed scheme in [31], [32] and [33] and compares the total storage burden of them. According to Table 2, our proposed protocol has dramatically improved the usage of storage space in the SM side.

TABLE 2. Total storage burden for each smart meter.

Schemes	Stored Parameters	Storage Burden
Scheme [31]	tl	$4\ KB$
Scheme [32]	X, H	$288\ B$
Scheme [33]	i, H, HD	$290\ B$
Our Scheme	$2 * H$	**$64\ B$**

TABLE 3. Total communication overhead comparison for each protocol execution.

	Scheme [31]	Scheme [32]	Scheme [33]		Ours	
	BC*	BC	BC	UC*	BC	UC
H	10	1	2	1	2	2
C	-	-	1	-	-	-
R	-	-	-	-	-	-
BF	-	-	1	-	-	-
HD	-	-	-	-	-	-
y	-	1	-	-	-	-
w	-	1	-	-	-	-
i	-	-	1	1	-	-
m	1	1	1	-	1	-
TS	-	-	-	-	1	1
ID	-	-	-	1	-	1
r	-	-	-	-	1	-
Total	2688 b	3200 b	1362 b		**944 b**	

*BC=Broadcast and *UC=Unicast

B. COMMUNICATION OVERHEAD

The total communication overhead of the proposed scheme in this paper is sum of all the communicated messages in both broadcast and unicast phases between SMs and NG. The communication overhead in each communication for the broadcast part is $\max\left\{\left(|m_i| + |V_i| + \left|TS^{NG}\right|\right), (|r_i| + |K_i|)\right\} = 400\ bit$, and for the unicast phase is $\left(\left|ID^j\right| + \left|E_i^j\right| + \left|V_i^{\prime j}\right| + \left|TS^{SM_j}\right|\right) = 544\ bit$. Hence, the overall communication overhead of the proposed scheme is $944\ bit$. Table 3 presents the number of each parameters which are sent in one run of the protocol in each communication for proposed schemes in [31]–[33] and compares the overall communication overhead of our proposed scheme with them. It is worth noting that in scheme TSV [31] NG choses k smart meters whom it wants to be able to verify the signature, and then broadcasts the packet through the network where no other entity except those designated SMs can verify the message. However, for having a meaningful comparison we considered $k = 10$.

TABLE 4. Execution time of cryptographic operations on a single core 798 MHz CPU and 256 MB of RAM.

Cryptographic Operation	Execution Time
SHA-256 Hash Function	25.97 μs
BCH Decoding Algorithm	3.31 ms
Exponential Operator	58.24 ms
128-bit Arbiter PUF	119.89 μs

TABLE 5. Daily computational cost of *SM*'s for time interval of fifteen minutes.

Cost	[31]	[32]	[33]	Ours
T_h	2016	192	672	384
T_{Decode}	×	×	96	×
T_{Exp}	×	96	×	×
T_{PUF}	×	×	192	×
Total (ms)	52.36	5596.03	358.13	**9.57**

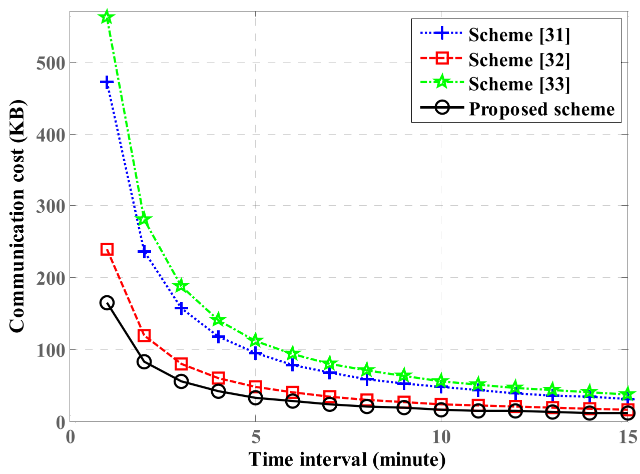


FIGURE 5. Daily communication overheads for different time intervals from one minute to fifteen minutes.

According to this table, although the proposed scheme in this paper is the only scheme, which provides two-way communication and data transmission simultaneously, it still has the lowest communication overhead. Furthermore, Fig. 5 depicts the total communicational cost of the mentioned schemes for different time intervals from one minute to fifteen minutes. According to this figure, the proposed scheme in this paper outperforms the other mentioned schemes for the short time intervals.

C. COMPUTATIONAL COST

As expected from a next-generation smart grid, the SMs are assumed as resources constrained devices while NG is

TABLE 6. Features-based comparison between the proposed scheme and other mentioned methods.

	Data report transmission	Two way communication	Mutual authentication	Presenting formal security proof	Fresh key for each authentication	Super lightweight design	Communication type	Design complexity level	Total implementation cost
Fouda et al.'s scheme [5]	**Yes**	No	No	**Yes**	No	No	UC	high	high
Mahmood et al.'s scheme [6]	**Yes**	No	No	**Yes**	No	No	UC	high	high
Uludag et al.'s scheme [7]	**Yes**	No	No	**Yes**	No	No	UC	high	high
Kaveh et al.'s scheme [8]	**Yes**	No	**Yes**	**Yes**	**Yes**	No	UC	medium	high
Li et al.'s scheme [19]	**Yes**	No	No	No	No	No	UC	high	high
Liu et al.'s scheme [20]	**Yes**	No	No	No	No	No	UC	high	high
Abbasinezhad-Mood et al.'s scheme [21]	**Yes**	**yes**	No	**Yes**	No	**Yes**	UC	**low**	medium
Li et al.'s scheme [31]	No	No	No	No	No	No	**BC**	medium	medium
Delavar et al.'s scheme [32]	No	No	No	No	No	No	**BC**	high	medium
Ameri et al.'s scheme [33]	No	No	No	**Yes**	**Yes**	No	**BC**	high	medium
Our proposed scheme	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**BC**	**low**	**low**

considered as a server with very high computational power. Thus, only the computational overhead for the SMs is studied. However, the proposed scheme in this paper imposes a reasonable computational cost in the NG side. For measuring the cost of different cryptographic operations on SMs, the advantage of JCE library [34] on a single core 798 MHz CPU and 256 MB of RAM is used that is very similar to a real-life smart meter [35]. In order to compute the cost of a PUF operation in scheme [32], the implementation result of [36] is used which a 128-bit arbiter PUF is implemented on an MSP430 micro-controller. In addition, the BCH encoding and decoding algorithms in the code-offset mechanism are used for correcting the PUF response errors [37]. The execution time for various cryptographic operation is shown in Table 4. It is worth noting that for each cryptographic operator, we have recorded the time of one thousand different executions on the mentioned hardware with a negligible standard deviation, and then we have put the average of these run-times in Table 4.

Table 5 shows the number of usage of the different cryptographic operators in one execution of protocol by each scheme and the total daily computational cost of each scheme for time interval of fifteen minutes. In this table, T_h, T_{Decode}, T_{Exp}, and T_{PUF} represent the execution time of one-way hash function (SHA-256), BCH decoding algorithm, exponential operation, and 128-bit arbiter PUF, respectively. As seen in section II, in our scheme, SM_j only uses four one-way hash functions for each run of protocol, which leads to decreasing of the computational cost significantly. The total daily computational cost of our scheme is $(4 \times 96 \times 0.026) \approx 9.984$ ms. According to the results shown in Table 5, the proposed protocol in this paper significantly improves computational overhead (more than five

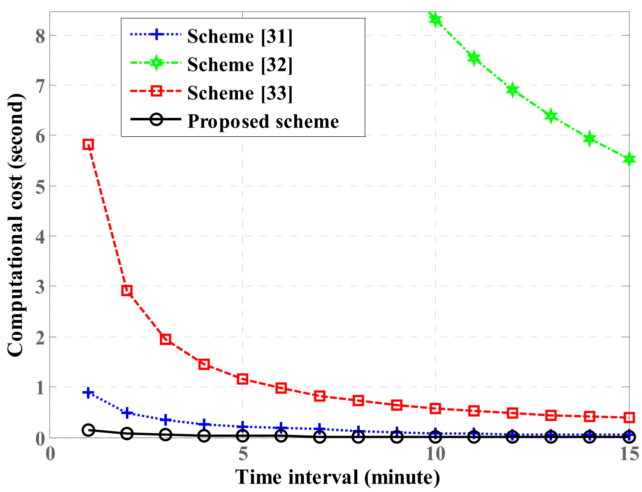


FIGURE 6. Daily computational cost for different time intervals from one to fifteen minutes.

times faster than the best previous method). Furthermore, Fig. 6 shows that our proposed protocol has the best computational cost for the time intervals from one minute to fifteen minutes.

According to the presented results in this section, the proposed protocol in this paper significantly improves the storage burden and computational cost of the smart meters, and also has the best performance in communication overhead. Furthermore, apart from this great performance, our proposed protocol is the only scheme, which supports two-way communication and confidentiality of transmitted messages between SMs and NG. As a result, because of dramatically improving of computational costs (especially in short time intervals) and storage burden, the proposed scheme in this paper can be considered as a practical candidate for near future of the smart grid, providing real-time authentication and two-way communication alongside the compatibility for the networks with very resource constrained devices.

Table 6 shows a feature-based comparison between our scheme and other mentioned broadcast and unicast schemes in section I, in both terms of security and efficiency. It is worth mentioning that, lightweight design relates to the communication, storage and computational overheads that schemes impose on the smart meters. The design complexity level is related to the cryptographic primitives implemented in smart meters in each scheme. For example, in our scheme the smart meters only use hash functions and logical XORs which make the implementation very simple while other schemes use primitives like exponential operators, PUF, or fuzzy extractors, which lead to more costly implementations. Needless to say, in comparison with unicast communication schemes, broadcast schemes have lower communicational and implementation expenses especially in networks with high number of receivers. As a result, the combination of design complexity of the schemes, the communication type they use, and their lightweight design, results to the total implementation expenses. According Table 6, the proposed scheme in this paper provides different important security and efficiency features for the *NAN* communication system of the smart grid.

VI. CONCLUSION

This paper proposed a very efficient authentication scheme for *NAN* communication system of smart grid. The proposed scheme used a broadcast and unicast technique for *NG* to *SM* and *SM* to *NG* data transmission, respectively. The security analysis showed that the proposed scheme is secure against the possible existing cyber-attacks. Furthermore, the formal security analysis proved the security of the protocol against the chosen message attack. Moreover, the performance evaluation analysis showed the intense efficiency of our protocol compared with the state-of-the-art in terms of storage burden and computational cost. As a result, because of the efficiency of the proposed scheme and the interesting features it provides, it can be considered as a proper security protocol for the networks with resource-constrained devices like smart grid.

ACKNOWLEDGMENT

This publication reflects the views only of the author and the commission cannot be held responsible for any use, which may be made of the information contained therein.

REFERENCES

[1] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart transmission grid: Vision and framework," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 168–177, Sep. 2010.

[2] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[3] C. Kalalas, L. Thrybom, and J. Alonso-Zarate, "Cellular communications for smart grid neighborhood area networks: A survey," *IEEE Access*, vol. 4, pp. 1469–1493, 2016.

[4] X. Lu, W. Wang, and J. Ma, "An empirical study of communication infrastructures towards the smart grid: Design, implementation, and evaluation," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 170–183, Mar. 2013.

[5] 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.

[6] 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," *Comput. Electr. Eng.*, vol. 52, pp. 114–124, May 2016.

[7] 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.

[8] 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.*, early access, Mar. 13, 2020, doi: 10.1109/JSYST.2019.2963235.

[9] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient design and hardware implementation of a secure communication scheme for smart grid," *Int. J. Commun. Syst.*, vol. 31, no. 10, p. e3575, Jul. 2018.

[10] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4815–4828, Nov. 2018.

[11] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in VANETs–An efficient and privacy-preserving cooperative downloading scheme," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1191–1204, Jun. 2020.

[12] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient design and extensive hardware evaluation of an anonymous data aggregation scheme for smart grid," *Secur. Privacy*, vol. 1, no. 2, p. e24, Mar. 2018.

[13] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, early access, Mar. 11, 2019, doi: 10.1109/TDSC.2019.2904274.

[14] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and extensive hardware performance analysis of an efficient pairwise key generation scheme for smart grid," *Int. J. Commun. Syst.*, vol. 31, no. 5, p. e3507, Mar. 2018.

[15] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, "Design of an anonymous lightweight communication protocol for smart grid and its implementation on 8-bit AVR and 32-bit ARM," *Int. J. Netw. Secur.*, vol. 21, no. 4, pp. 607–617, 2019.

[16] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[17] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1495–1502, Mar. 2020.

[18] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and microcontroller-based hardware performance analysis of a security-enhanced lightweight communication scheme for smart grid," *Secur. Privacy*, vol. 1, no. 5, p. e34, 2018.

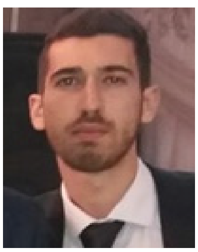
[19] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.

[20] 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.

[21] 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, doi: 10.1109/TSG.2017.2705763.

[22] S. Aghapour, M. H. Ameri, and J. Mohajeri, "A multi sender attribute-based broadcast authentication scheme," in *Proc. 8th Int. Symp. Telecommun. (IST)*, Sep. 2016, pp. 78–83.

[23] Y. Ding, Y.-C. Tian, X. Li, Y. Mishra, G. Ledwich, and C. Zhou, ''Constrained broadcast with minimized latency in neighborhood area networks of smart grid,'' *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 309–318, Jan. 2020.
[24] A. A. Yavuz, ''An efficient real-time broadcast authentication scheme for command and control messages,'' *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1733–1742, Oct. 2014.
[25] X. Li, Y.-C. Tian, G. Ledwich, Y. Mishra, X. Han, and C. Zhou, ''Constrained optimization of multicast routing for wide area control of smart grid,'' *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3801–3808, Jul. 2019.
[26] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, ''Smart grid communication: Its challenges and opportunities,'' *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 36–46, Mar. 2013.
[27] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, ''Toward unified security and privacy protection for smart meter networks,'' *IEEE Syst. J.*, vol. 8, no. 2, pp. 641–654, Jun. 2014.
[28] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, ''Application of big data and machine learning in smart grid, and associated security concerns: A review,'' *IEEE Access*, vol. 7, pp. 13960–13988, 2019.
[29] P. Eder-Neuhauser, T. Zseby, and J. Fabini, ''Resilience and security: A qualitative survey of urban smart grid architectures,'' *IEEE Access*, vol. 4, pp. 839–848, 2016.
[30] B. Jimada-Ojuolape and J. Teh, ''Impact of the integration of information and communication technology on power system reliability: A review,'' *IEEE Access*, vol. 8, pp. 24600–24615, 2020.
[31] Q. Li and G. Cao, ''Multicast authentication in the smart grid with one-time signature,'' *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686–696, Dec. 2011.
[32] M. Delavar, S. Mirzakuchaki, M. H. Ameri, and J. Mohajeri, ''PUF-based solutions for secure communications in advanced metering infrastructure (AMI),'' *Int. J. Commun. Syst.*, vol. 30, no. 9, p. e3195, 2017.
[33] 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.
[34] Oracle Technology Network. *Java Cryptography Architecture*. Accessed: Nov. 20, 2019. [Online]. Available: http://docs.oracle.com/javase/6/docs/technotes/guides/crypto/CrypoSpec.html
[35] *Atmel's Family of Smart Power Meters*. Accessed: Nov. 20, 2019. [Online]. Available: https://www.microchip.com/design-centers/smart-energy-products/metering
[36] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, ''Physical unclonable functions and applications: A tutorial,'' *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
[37] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, ''Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,'' *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.



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 Nowshahr Marine Science University 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 physically unclonable functions (PUFs), cryptographic protocols, smart grid and the IoT security, and machine learning.

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

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 (a Full Professor) with the Department of Electrical Engineering, IUST. He is the author of more than 400 scientific publications in journals and international conferences in addition to 11 academic books. His research interests include circuits and systems design. He is also the Editor-in-Chief of the *Iranian Journal of Marine Technology* and an Editorial Board Member of the *Iranian Journal of Electrical and Electronic Engineering*.