A novel multi-stage distributed authentication scheme for smart meter communication

Manjunath Hegde[1], Adnan Anwar[2], Karunakar Kotegar[1], Zubair Baig[2] and Robin Doss[2]

[1] Department of Computer Applications, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India
[2] School of IT, Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, VIC, Australia

Corresponding author
Adnan Anwar,
adnan.anwar@deakin.edu.au

ABSTRACT

Smart meters have ensured effective end-user energy consumption data management and helping the power companies towards network operation efficiency. However, recent studies highlighted that cyber adversaries may launch attacks on smart meters that can cause data availability, integrity, and confidentiality issues both at the consumer side or at a network operator's end. Therefore, research on smart meter data security has been attributed as one of the top priorities to ensure the safety and reliability of the critical energy system infrastructure. Authentication is one of the basic building blocks of any secure system. Numerous authentication schemes have been proposed for the smart grid, but most of these methods are applicable for two party communication. In this article, we propose a distributed, dynamic multistage authenticated key agreement scheme for smart meter communication. The proposed scheme provides secure authentication between smart meter, NAN gateway, and SCADA energy center in a distributed manner. Through rigorous cryptanalysis we have proved that the proposed scheme resist replay attack, insider attack, impersonation attack and man-in-the-middle attack. Also, it provides perfect forward secrecy, device anonymity and data confidentiality. The proposed scheme security is formally proved in the CK—model and, using BAN logic, it is proved that the scheme creates a secure session between the communication participants. The proposed scheme is simulated using the AVISPA tool and verified the safety against all active attacks. Further, efficiency analysis of the scheme has been made by considering its computation, communication, and functional costs. The computed results are compared with other related schemes. From these analysis results, it is proved that the proposed scheme is robust and secure when compared to other schemes.

INTRODUCTION

The smart grid is one of the critical infrastructures for any nation. The traditional energy system equipped with advanced sensing, communication and control technologies transforms the decades old power system into a smart grid. While the smart grid provides a wide range of utilities and help the end-users to improve their lifestyle and minimize the

cost of energy, new types of cyber-threats have emerged. According to a recent report published by Kaspersky, a noticeable number of cyber incidents were reported in the energy control centres (In H1 2020, ICS computers blocked 32.6% malicious contents) that has raised a major concern (*Kaspersky ICS CERT, 2020*). For example, a ransomware attack on a large Portuguese energy company was claimed to have stolen around 10TB of sensitive information. As per the report, the major categories of the cyber attacks experienced by the industrial control centre (ICS) of the energy system are worms, spyware and cryptocurrency miners. If not detected, these cyber attacks and new sophisticated threats can cause significant damage to the physcial assets, financial losses, and may even create catastrophic cascading failures. Hence, a good number of research is going on towards the investigation of emerging attacks and threat models (*Anwar, Mahmood & Pickering, 2016*; *Anwar, Mahmood & Pickering, 2017*; *Anwar, Mahmood & Ahmed, 2015*) for the energy system and possible countermeasures (*Yang et al., 2014*; *Anwar, Mahmood & Tari, 2015*).

In recent years, smart meters (SM) have been widely deployed to monitor energy usages of the end-user's consumption data. For example, smart meters have been installed in all residential homes across Victoria, which is one of the major Australian states (*DELWP, 2020*). SMs have provided the customers insights on their consumption profile and opened the door for data driven informed decision making and control energy at a household level. However, SM data communication is based on wireless medium and making the use of internet technologies. Wireless communication model for SM data transmission may allow malicious attackers to perform various attacks if they do not have a robust security system (*Gope & Sikdar, 2018*). If the system is compromised by an adversary, the attacker can eavesdrop and modify the communication data. This kind of attack is data privacy and confidentiality attack. Also, the attacker can interrupt the transmitted messages or cause a Denial of Service (DoS) and/or jamming attack against the system that may lead to a data availability attack. Moreover, a new type of attack has emerged where the attacker can inject malicious or false information into the smart meter data payloads and corrupt the original information (*Anwar, Mahmood & Tari, 2015*). This kind of attack is known as a data integrity attack against smart meters within an advanced metering infrastructures. Hence, attacks on smart meter can impact on the Confidentiality, Integrity and Availability (CIA) triad of an energy systems demand side management. Therefore, the security issues have been highlighted as a major concern of today's smart grid smart meter communication and data management (*Aziz et al., 2019*; *Ni & Paul, 2019*; *Anwar, Mahmood & Tari, 2017*). Hence, it is necessary to build a powerful security framework for the smart grid system.

Authentication is one of the primary and recommended approaches to address smart grid smart meter communication security issues. In this paper, we have proposed a novel distributed multi-stage authentication scheme for smart grid smart meter communication. There are numerous authentication schemes for smart grid are proposed in recent years. The need for the proposed authentication scheme is that there are drawbacks identified in most of the recently proposed schemes and they fail to achieve security requirements (*Zhang et al., 2019*). We have listed the potential vulnerabilities

which restrict to the providing of secure authentication in the smart grid smart meter communication. Some of the notable drawbacks are: (i) Anonymity and untraceability which is one of the hurdles to achieve the secure authentication. It enables to reveal the identity of the smart meter which holds the partial information of the login message. Also, an unauthorized user may compromise a meter from the physical box and control the home appliances (*Kumar et al., 2019*). (ii) The smart meter sends unit consumption data periodically: 15/30/60 minutes. The participants involved in the smart grid smart meter communication are connected via the network *Kumar et al. (2018)*. Since the communication has been done through the open channel, the adversary can intercept the network to leak, modify or delete data (*Wang & Lu, 2013*). Communication interception may leads towards man in middle attack, replay attack and so on.

In smart energy networks, power transmission and distribution system is separated from the data communication network (*Fouda et al., 2011*). In power transmission and distribution system, electricity is delivered from the power plant to end-users. In this paper, we described the network from the data communications point of view. The detailed system design is illustrated in the "System Model". Traditionally, the Supervisory Control and Data Acquisition (SCADA) system has been used to monitor and control the power grid. The SCADA system is a centralized system, where the substations are connected to a control center. The centralized structure of the SCADA system limits its scalability and makes its applicability only for local monitoring. But, an extended SCADA system makes it to Wide-area monitoring, protection, and control system (*Shin, He & Zhang, 2014*; *Eder-Neuhauser, Zseby & Fabini, 2016*). Here, smart grid topology is split into a number of networks (*Zhong, Chim & Hui, 2015*). The active participants in the communication are the smart meter (SM), home area network (HAN), neighbourhood area network gateway (NANG) and the SCADA control center/server. These participants are organized in a hierarchical structure for smart grid communications. To implement the mutual authentication between the active participants, several schemes depending upon the trusted third party (*Li et al., 2013*; *Li et al., 2017*; *Wu et al., 2019*). Dependency on the third party always a bottleneck for the system efficiency when it is too busy on handling of large incoming requests (*Odelu et al., 2017*). Also, a trusted third party should be suitable to adopt communication environment (*Irshad et al., 2020*). The authentication schemes independent of the trusted third party assumed that the network between NANG and SCADA control server is secure (*Li et al., 2019*; *Kumar et al., 2019*). Since the communication between NANG and SCADA control center/server will be done in an open channel, there will be the chances for network interception. Therefore, it is necessary to propose a novel distributed authentication scheme, which is independent from the third party and authenticate all active participants involved in the communication. Hence, the contributions of the proposed scheme are:

- We have proposed a novel distributed dynamic multistage authenticated key agreement scheme to achieve the illustrated security problems. The proposed scheme provides secure authentication between SM, NANG, and SCADA control server in a distributed

manner, which means the authentication of SM, NANG, and SCADA control server does not depending upon any third party.

- The proposed scheme achieves the authentication in a fully hierarchical manner which is suitable for smart grid smart meter communication architecture.
- The proposed security scheme is formally proved in the CK - model. The scheme is simulated using AVISPA tool to verify the security against all active attacks.
- The proposed scheme's efficiency analysis has been made, considering its computation, communication, and functional costs. The computed results are compared with the other related schemes.

Related work

Authentication is a fundamental security solution and it has been extensively studied in various application areas. In smart grid smart meter communication, several authentication schemes have been proposed by numerous researchers. Even after the schemes are developed for specific architecture or application, there may be some similarities observed in terms of authentication factors, cryptographic operation, and message communication (*Abbasinezhad-Mood, Ostad-Sharif & Nikooghadam, 2019*). In this article, we only reviewed recent and relevant literatures, for the most part, authentication which focuses on the network architecture which includes SM, NAN, and SCADA control server. *Wu & Zhou (2011)* proposed an anonymous key distribution scheme for the smart grid. This scheme mainly combines the symmetric key and elliptic curve public key techniques. In the scheme, the symmetric key was based on the Needham-Schroeder authentication protocol. *Wu & Zhou (2011)* claimed that the proposed scheme effectively resists the man-in-the-middle attack and the replay attack. Later, *Xia & Wang (2012)* analysed *Wu & Zhou's (2011)* scheme and identified the scheme is vulnerable to man-in-the-middle attack. To overcome the identified attack, *Xia & Wang (2012)* proposed a key distribution scheme. Here, the authors used a trusted third party to manage the key distribution for the smart meter and the service provider.

Nicanfar et al. (2013) proposed an efficient mutual authentication scheme. This scheme was developed to authenticate the entities that present outside of the home area network. *Nicanfar et al. (2013)* assumed that the authenticating participants are a smart meter and authentication server. From this literature, *Nicanfar et al. (2013)* also proposed a key management protocol based on identity cryptography for secure smart grid communications using the public key infrastructure. *Li et al. (2013)* proposed a Merkle-Tree-Based authentication scheme for secure smart grid communication. This article is more focused on eliminating message injection, message analysis, message modification, and replay attacks during communication.

Tsai & Lo (2015) reviewed *Xia & Wang's (2012)* authentication scheme and identified that *Xia & Wang (2012)* scheme does not support smart meter anonymity and perfect forward secrecy. To overcome the identified weaknesses, *Tsai & Lo's (2015)* proposed a key distribution scheme for smart grid environments. The scheme was proposed including properties of bilinear pairings. Importantly, *Tsai & Lo's (2015)* scheme needed a trusted

third party to distribute the private keys for smart meters and smart grid during registration. Later, *Odelu et al. (2016)* reviewed *Tsai & Lo's (2015)* scheme and found that the scheme can reveal the smart meter's secret credentials when the secret key has been revealed. To overcome the identified security weakness, *Odelu et al. (2016)* proposed a new authenticated key agreement scheme based on bilinear pairings for the smart grid. Like *Tsai & Lo (2015)* scheme, *Odelu et al. (2016)* utilized trusted third party to handle the private keys.

Further, *Mahmood et al. (2016)* proposed a hybrid Diffie-Hellman based lightweight authentication scheme using AES and RSA cryptography. This scheme was focused on achieving authentication between building area networks (BAN) and smart meters. The objective of the scheme was to avoid replay attack during authentication. *Wazid et al. (2017)* proposed a three-factor user authentication scheme for a renewable energy-based smart grid environment. Here, the objective was to authenticate vehicle user who wants to charge his/her electric vehicle battery. In this scheme, even though there are multiple authorities involved, authentication can be possible only between user and smart meter. Also, *Wazid et al.'s (2017)* scheme is dependent on trusted authority for smart meter registration.

Mahmood et al. (2018) proposed a lightweight ECC-based authentication scheme for smart grid communication. The aim of the scheme is to authenticate two registered users communicating in the environment. In this scheme, the trusted third party was responsible to generate preliminary parameters like selecting elliptic curve, random base point, one-way hash functions, secret key, and so on. *Mahmood et al.'s (2018)* scheme was also aimed to eliminate the trade-off between performance and security in smart grid communication where the scheme should provide high security with high performance. Further *Abbasinezhad-Mood & Nikooghadam (2018)* analyzed *Mahmood et al.'s (2018)* scheme and identified that the scheme cannot provide the perfect forward secrecy. Also identified that the private key of users and shared session keys can be easily compromised with an adversary. To overcome the identified weaknesses, *Abbasinezhad-Mood & Nikooghadam (2018)* proposed elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Mahmood et al.'s (2018)* scheme was also reviewed by *Chen et al. (2019)* and identified that the scheme could not provide the perfect forward secrecy and private key privacy. Also, the authors analyzed *Abbasinezhad-Mood & Nikooghadam's (2018)* scheme and identified that the scheme is vulnerable to the replay attack. To withstand the identified weaknesses, *Chen et al. (2019)* proposed a bilinear map pairing-based authentication and key establishment scheme.

Zhang et al. (2019) proposed a lightweight anonymous authentication and key agreement scheme for the smart grid. This scheme allows the smart meter and the service provider to authenticate each other. The authentication scheme does not follow any hierarchical network architecture which minimizes the system applicability. *Ma et al. (2019)* proposed the eye-movement and iris recognition based portable remote authentication for the smart grid. It was a biometrics-based remote operator authentication scheme that uses the record of eye-movement trajectory and randomly selected iris image for authentication.

Recently, *Moghadam et al. (2020)* proposed a lightweight key management protocol for secure communication between substation and data center in smart grids. The scheme was based on hash functions and private keys. *Irshad et al. (2020)* proposed a message authentication scheme for secure communications between HAN gateway and BAN gateway in smart grids. *Aghapour et al. (2020)* proposed a broadcast authentication scheme for smart grid communications which uses hash functions and private key. Here, the authentication was to be done between the NAN gateway and the smart meter. *Sadhukhan et al. (2020)* proposed a privacy-preserving authentication scheme for smart-grid communication using elliptic curve cryptography. Here, the scheme can authenticate HAN gateway and BAN gateway in smart grids. This scheme needs a trusted third party to generate credentials, keys, and hash functions. *Wu et al. (2021)* reviewed *Chen et al.'s (2019)* scheme and identified the known session-specific temporary information attack where adversary can get the information of random nonce which needed to compute the session key. Also, *Wu et al. (2021)* identified that *Chen et al.'s (2019)* scheme is vulnerable to impersonation attack. To overcome identified weaknesses, *Wu et al. (2021)* proposed an improved pairing-based authentication scheme. The proposed scheme, depended upon a trusted third party to generate secret keys, cyclic groups, and hash functions.

From the above literature study we can observe that (i) most of the authentication schemes have security flaws and their improvements are also show some possible attacks. (ii) Many schemes can perform authentication either between the smart meter and NAN gateway or gateway and SCADA center. (iii) Also, the authentication schemes that implemented to the hierarchical network are dependent upon a trusted third party. Therefore, It is vary much necessary to propose an authentication scheme that can mutually authenticate smart meter, NAN gateway, and SCADA center without involvement of any third party. Hence, we have proposed a novel multistage distributed authentication scheme for smart grid communication.

The rest of the article is assembled as follows. "System Model" presents the system model used to propose the authentication scheme. "Cryptographic Preliminaries" discusses the necessary cryptographic preliminaries to understand the scheme. "The Proposed Scheme" illustrates the proposed multi-stage authentication scheme for smart meter communication. This section includes a detailed explanation of the steps of authentication in each phase. Further, "Cryptanalysis of the Proposed Scheme" presents the cryptanalysis of the proposed scheme. Here, we proved the data confidentiality, sensitivity and the security provided in the proposed scheme. The formal security verification of the proposed scheme based on the CK adversary model is illustrated in "Formal Security Proof", followed by the results of formal security verification using AVISPA are presented in "Result of Formal Security Verification Using Avispa Tool". "Efficiency Analysis" discusses the proposed scheme's efficiency analysis by comparing result computation cost ("Computation Cost Analysis") and communication cost ("Communication Cost") of the proposed scheme with the other related schemes. This section also gives the comparison result of the essential functionalities ("Functional analysis") in smart meter communication. Finally, the article depicts the concluding remarks.

SYSTEM MODEL

In this section, we present the system model which involves key components towards a smart meter communication between the consumers and SCADA control centres. As discussed in the "Introduction", the system model described in the article is from the data communications point of view. The active participants are Smart Meter (SM), Home Area Network (HAN), Neighborhood Area Network Gateway (NANG) and SCADA control center/Server. These participants are well connected in a hierarchical manner. In the considered system architecture, HAN has been considered as the bottom layer. Within a HAN, home appliances are connected to a Smart Meter (SM). The purpose of SM is to collect the aggregated consumption (e.g., dishwasher, electric oven, etc) and generation (e.g., solar PV) profiles of the home devices. The collected data can be transferred to the SCADA control center/Server or smart grid (SG) for data storage and analysis. The communication happens via NANG that has been considered as the middle layer of the system. The complete system architecture is presented in Fig. 1.

CRYPTOGRAPHIC PRELIMINARIES

This section discusses the cryptographic preliminaries necessary to understand the proposed scheme. The necessary encryption/decryption operations are done using Elliptic Curve Cryptography (ECC). The security strength of ECC relies heavily on the hardness of solving the elliptic curve discrete logarithm problem (ECDLP). Compared to any other public-key cryptosystems, ECC can provide significant security strength to any communication system with less key size (*Hancock, 2001*). This property reduces the algorithmic computational cost and makes the protocol more lightweight.

Elliptic curve cryptography: The equation of the elliptic curve $E_p(a, b)$ over F_p ($p > 3$ and is a large prime number) is defined as $y^2 \ mod \ p = (x^3 + ax + b) \ mod \ p$ where $(4a^3 + 27b^2)$ $mod \ p = 0$; $x, y, a, b \in [0, p-1]$. Any points $(x, y) \in E_p(a, b)$ are denoted as $E(F_p) = \{(x, y) : x,$ y in F_p satisfy $y^2 = (x^3 + ax + b)\} \cup \mathcal{O}$ where $\mathcal{O}$ is a point at infinity. The point multiplication is computed by repeated addition as $k.P = P + P + P + ….. + P$ K times (*Koblitz, 1987*).

Elliptic Curve Discrete Logarithm Problem(ECDLP): An elliptic curve E defined over a finite field $GF(q)$ and two points P, Q $\in$ E, it is hard to find an integer x $\in Z_p^\star$ such that Q = xP.

Elliptic Curve Diffie Hellman (ECDH): Elliptic Curve Diffie Hellman (ECDH) key exchange is the the classical Diffie-Hellman key exchange which exchanges secret information or secure keys between two parties. The keys are exchanged between A and B as follows.

System selects an elliptic curve E_p over the prime finite field F_p where p is a large prime number and select a point on elliptic curve P of order n. The algorithm is as follows.

1. *A* generates a random number k_A in the interval [1, $n-1$] and performs a scalar multiplication $Q_A = k_A \times P$ Then, sends Q_A to *B*

2. *B* also generates a random number k_B and computes $Q_B = k_B \times P$ by scalar multiplication in the same way as described above and sends Q_B to A.
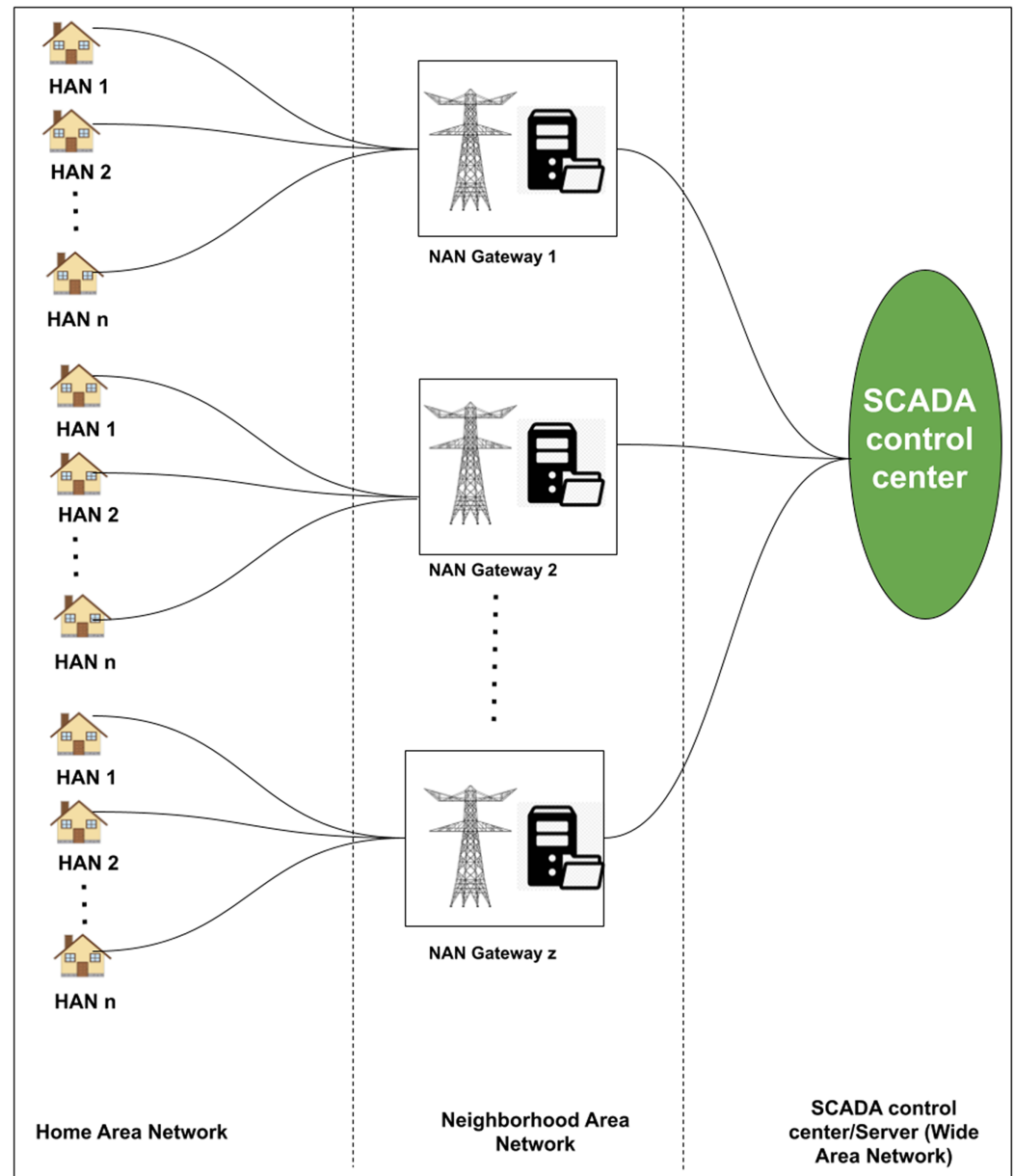
Figure 1 Proposed architecture of the system model.

3. After receiving Q_B from B, A computes $K_1 = k_A \times Q_B$. Similarly, B receives Q_A from A and computes $K_2 = k_B \times Q_A$.

4. A and B shares K_1 and K_2 between them. Thus, two entities exchanges the keys securely.

THE PROPOSED SCHEME

This section presents the proposed novel distributed dynamic multistage authenticated key agreement scheme for the smart grid. The proposed scheme contains three phases (1) Initialization phase, (2) Registration phase and (3) Authentication phase. The notations used throughout the scheme are presented in Table 1.

Table 1 Notations and descriptions.

Notations	Descriptions
SG_i	SCADA control center/server
SM_i	Smart meter
E_p	Elliptic curve of order p
F_p	Finite field
$NANG_i$	Neighborhood area network gateway
P	Point on elliptic curve E_p
s, P_{pub}	Private/public key pair of SG_i where $P_{pub} = s.P$
PW_i	Password of U_i
+	Bitwise XOR operator
||	Concatenation operator
$h_0(.), h_1(.), h_2(.)$	One-way hash functions
T_1, T_2, T_3, T_4	Timestamps generated by $SM_i, NANG_i, SG_i$

Initialization phase

To fully describe the proposed scheme, the process of system initialization is explained first. The initialization has to be done while deploying the system. It includes selecting an elliptic curve, hash functions, public and private keys necessary to perform encryption/decryption, and hashing operation throughout the entire scheme.

SG_i choose an elliptic curve E_p over the finite field F_p where p is a large prime number. SG_i also selects an elliptic curve point P of order n and one way hash functions $h_0(.) \rightarrow Z^*, h_1(.) \rightarrow Z^*, h_2(.) \rightarrow Z^*$. Further SG_i picks the private key x and computes the public key $P_{pub} = x.P$. Finally, SG_i publishes the parameters $\{E_p, P, F_p, h_0(.), h_1(.), h_2(.), P_{pub}\}$.

Registration phase

The registration phase includes steps to register participants (e.g., $SM_i, NANG_i$, etc.), which take part in the system. This phase includes the registration of Neighborhood Area Network gateway $NANG_i$ and smart meter SM_i. The details of $NANG_i$ and SM_i registration have been presented below.

NAN gateway registration phase

In the proposed scheme, $NANG_i$ registration is done with a SCADA control center/server. The steps involved in the $NANG_i$ registration have been illustrated as follows:

- $NANG_i$ selects NID_i, b_j and computes $A_i = h_0(NID_i || b_j)$
- Sends the registration request message $\{NID_i, A_i\}$ to the SG_i.
- SG_i receives the request message, generates the random number e and computes

$m_i = h_0(s || e)$,
$V_n = h_0(m_i || A_i).P_{pub}$ and
$H_n = h_0(V_n || NID_i)$

Table 2 NAN gateway registration phase.

NAN gateway	SCADA control center/server
Selects NID_i, b_j	
Computes $A_i = h_0(NID_i\| b_j)$	
Sends $\{NID_i, A_i\}$	
$\{NID_i, A_i\}$ $----\rightarrow$	
	Receives message and generates the random number e
	Computes $m_i = h_0(s\| e)$
	$V_n = h_0(m_i \|A_i).P_{pub}$ and
	$H_n = h_0(V_n \|NID_i)$
	Stores H_n into the database and sends V_n to the $NANG_i$
	$\{V_n\}$ $\leftarrow--$
Receives V_n and stores $\{NID_i, b_j, V_n\}$	

- SG_i stores H_n into the database and sends V_n to the $NANG_i$. NAN gateway receives V_n and stores $\{NID_i, b_j, V_n\}$ into its database. The registration phase of NAN gateway has been presented in the Table 2.

Smart meter registration phase

The registration of the SM_i is with $NANG_i$. The registration of SM_i has been presented below:

- SM_i selects MID_i, b_i, computes $A_j = h_0(MID_i \|b_i)$ and sends the registration request message $\{MID_i, A_j\}$ to the NAN gateway.

- $NANG_i$ receives the request message and computes

$H_n = h_0(V_n \|NID_i)$,
$V_m = h_0(H_n \|A_j).P_{pub}$ and
$H_m = h_0(V_m\| MID_i)$

- $NANG_i$ stores H_m into the database and sends V_m to the SM_i. Smart Meter receives V_m and stores $\{MID_i, b_i, V_m\}$ into SM_i. The Smart meter registration phase has been presented in Table 3.

Authentication phase

The authentication phase is performed between SM_i, $NANG_i$, and SG_i. Here, SM_i and SG_i mutually authenticate through $NANG_i$. Table 4 presents the authentication phase of the proposed scheme. The steps involved in this phase are as follows:

- Smart meter SM_i generates a random number w and computes

$C_{sm} = w.P_{pub} \oplus h_0(V_m \|MID_i)$
$CID_i = h_1(w.P_{pub}\| T_1) \oplus b_i$
$C_1 = h_1(CID_i \|b_i \|w.P_{pub})$

Table 3 Smart meter registration phase.

Smart meter	NAN gateway
MID_i, b_i	
Computes $A_j = h_0(MID_i\, b_i)$	
Sends $\{MID_i, A_j\}$	
$\{MID_i, A_j\}$ $----\rightarrow$	
	Receives message
	Computes $H_n = h_0(V_n \,\|NID_i)$,
	$V_m = h_0(H_n \,\|A_j).P_{pub}$ and
	$H_m = h_0(V_m\| \, MID_i)$
	Stores H_m into its database and sends V_m to the SM_i.
	$\{V_m\}$ $\leftarrow--$
Receives V_m and stores $\{MID_i, b_i, V_m\}$ into SM_i.	

- Further SM_i send login request message $M_1 = \{C_{sm}, CID_i, C_1, T_1\}$ to NAN gateway.
- $NANG_i$ receives the message M_1 sent by SM_i and checks the validity. To verify the freshness of the received message, $NANG_i$ takes its current timestamp T_2 and checks that whether $T_2 - T_1 \le \delta\, T$ or not. Also, $NANG_i$ confirms that between the time $(T_1 + \delta\, T)$ and $(T_1 - \delta\, T)$ there were no other requests which contains same parameters of M_1 has not received. If these conditions are not true, then the system rejects the request message and drops the session.
- $NANG_i$ computes the following after receiving the login request message:

$$w.P_{pub} = C_{sm} \oplus H_m$$
$$bi = h_1(w.P_{pub} \,\|T_1) \oplus CID_i$$
$$C_{nan} = C_{sm} \oplus H_m \oplus h_0(V_n \,\|NID_i)$$
$$RID_s = h_1(C_{nan}\, h_0(V_n \,\|NID_i)) \oplus b_j$$
$$C_2 = h_1(C_1 \,\|T_2 \,\|C_{nan}\, b_j)$$

- $NANG_i$ Sends $\{CID_i, C_2, C_{nan}, RID_s, T_2, T_1\}$ to the server.
- SG_i receives the request message sent by NAN gateway and checks its validity to make sure that the request is made recently. SG_i takes its present timestamp T_3 and checks whether $T_3 - T_2 \le \delta\, T$. If the condition does not satisfy, then SG_i rejects the received message and drops the session. If not, SG_i begins the authentication process.
- Once the request message accepted by the sever, it starts authenticating it. To do that SG_i computes the following: $w.P_{pub} = C_{nan} \oplus H_n$

$$b_i = h_1(w.P_{pub}\| \, T_1) \oplus CID_i$$
$$b_j = h_1(C_n \,\|H_n) \oplus RID_s$$
$$C_1 = h_1(CID_i \,\|b_i \,\|w.P_{pub})$$
$$C_2 = h_1(C1 \,\|T_2 \,\|C_{nan} \,\|b_j)$$

Table 4 Login and authentication phase of the proposed scheme.

Smart meter	NAN gateway	SCADA control center/server
Generates w and computes		
$C_{sm} = w.P_{pub} \oplus h_0(V_m \|MID_i)$		
$CID_i = h_1(w.P_{pub}\| T_1) \oplus b_i$		
$C_1 = h_1(CID_i \|b_i\|w.P_{pub})$		
Sends $M_1 = \{C_{sm}, CID_i, C_1, T_1\}$ to NAN gateway.		
$\{M_1 = C_{sm}, CID_i, C_1, T_1\}$		
$\text{--------------}\rightarrow$		
	Receives the message sent and checks $T_2 - T_1 \leq \delta T$.	
	Computes	
	$w.P_{pub} = C_{sm} \oplus H_m$	
	$b_i = h_1(w.P_{pub}\| T_1) \oplus CID_i$	
	$C_{nan} = C_{sm} \oplus H_m \oplus h_0(V_n \|NID_i)$	
	$RID_s = h_1(C_{nan} \|h_0(V_n \|NID_i)) \oplus b_j$	
	$C_2 = h_1(C_1\| T_2\| C_{nan} \|b_j)$	
	Sends $\{CID_i, C_2, C_{nan}, RID_s, T_2, T_1\}$ to the SG_i.	
	$CID_i, C_2, C_{nan}, RID_s, T_2, T_1$	
	$\text{--------------}\rightarrow$	
		Receives the request message and checks whether $T_3 - T_2 \leq \delta T$.
		Computes the following:
		$w.P_{pub} = C_{nan} \oplus H_n$
		$b_i = h_1(w.P_{pub}\| T_1) \oplus CID_i$
		$b_j = h_1(C_n\| H_n) \oplus RID_s$
		$C_1 = h_1(CID_i\| b_i \|w.P_{pub})$
		$C_2 = h_1(C1\| T_2 \|C_{nan} \|b_j)$
		Checks $C_2 ? = C_2$ If both are equal then.
		Generates y and computes
		$C_s = y.P_{pub} \oplus h_2(H_n)$
		$SK_s = h_2(y.P_{pub}\| w.P_{pub} \|b_i \|b_j)$
		$C_3 = h_2(SK_s\| t_3 \|y.P_{pub})$
		Sends $M_2 = \{C_3, C_s, T_3\}$.
		$\{M_2 = C_3, C_s, T_3\}$
		$\leftarrow\text{----------}$
	Receives M_2 and computes	
	$y.P_{pub} = C_s \oplus h_2(h_0(Vn \|NID_i))$	
	$RID_m = h_2(C_m\| H_m) \oplus b_j$	
	$C_m = C_s \oplus H_m \oplus h_2(h_0(Vn\| NID_i))$	
	$SK_N = h_2(y.P_{pub} \|w.P_{pub} \|b_i \|b_j)$	
	$C_4 = h_2(C_3 \|T_4 \|C_m \|b_j)$	
	Sends $\{C_s, T_3, C_4, C_m, T_4, RID_m\}$ to the SM_i	
	$\{C_s, T_3, C_4, C_m, T_4, RID_m\}$	
	$\leftarrow\text{--------------}$	

Smart meter	NAN gateway	SCADA control center/server
Receives mutual authentication message and computes		
$y.P_{pub} = C_s \oplus h_0(V_m \| MID_i)$		
$b_j = h_1(C_m \| h_0(V_m \| MID_i)) \oplus RID_m$		
$SK_M = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$		
$C_3 = h_2(SK_M \| T3 \| y.P_{pub})$		
$C4 = h_2(C_3 \| T_4 \| C_m \| b_j)$		
Smart meter session key	NAN Gateway session key	Server session key
$SK_M = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$	$SK_N = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$	$SK_s = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$

- Server compares C_2 with received C_2. If both are equal then the server completes the authentication of SM_i and begins the mutual authentication.
- To perform mutual authentication, server first generates the random number y and computes $C_s = y.P_{pub} \oplus h_2(H_n)$

  $SK_s = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$
  $C_3 = h_2(SK_s \| t_3 \| y.P_{pub})$

- SG_i sends a mutual authentication message $M_2 = \{C_3, C_s, T_3\}$ to NAN gateway. $NANG_i$ receives M_2 and computes $y.P_{pub} = C_s \oplus h_2(h_0(V_n \| NID_i))$

  $RID_m = h_2(C_m \| H_m) \oplus b_j$
  $C_m = C_s \oplus H_m \oplus h_0(V_n \| NID_i)$
  $SK_N = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$
  $C_4 = h_2(C_3 \| T_4 \| C_m \| b_j)$
  Sends $\{C_s, T_3, C_4, C_m, T_4, RID_m\}$ to the SM_i

- Smart meter receives mutual authentication message from NAN gateway and computes

  $y.P_{pub} = C_s \oplus h_0(V_m \| MID_i)$
  $b_j = h_1(C_m h_0(V_m \| MID_i)) \oplus RID_m$
  $SK_M = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$
  $C_3 = h_2(SK_M \| T3 \| y.P_{pub})$
  $C4 = h_2(C_3 \| T_4 \| C_m \| b_j)$

- SM_i Compares C_4 with received C_4 if both are equal smart meter, NAN gateway, and the server establishes the connection successfully.
- Further communications will be done through the shared session keys. The session keys are For smart meter, $SK_M = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$

  For NAN gateway $SK_N = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$
  For Server $SK_s = h_2(y.P_{pub} \| w.P_{pub} \| b_i \| b_j)$.

CRYPTANALYSIS OF THE PROPOSED SCHEME

This section presents the cryptanalysis of the proposed multistage authentication scheme. This analysis helped us to prove the sensitivity of the obtained results where stored and communication parameters does not impact on the systems privacy and the security.

Resiliency against replay attack

Resiliency against replay attacks can be possible only when the server verifies the freshness of the login message before beginning the authentication. In the proposed scheme, a timestamp has been used to check the validity of the login request message. Suppose a participant receives the message contains timestamp T, then the participant takes its current timestamp T and checks the condition $T' - T \leq \delta T$. If this condition is satisfied, the next step would be to proceed else participant drops the session.

Let us assume that adversary steals the previous successfully authenticated login request message $\{C_{sm}, CID_i, C_1, T_1\}$ sent from SM_i to $NANG_i$ and $\{CID_i, C_2, C_{nan}, RID_s, T_2, T_1\}$ sent from $NANG_i$ to SG_i. Attacker trying perform replay attack by resending stolen login request message. Here, both $NANG_i$ and SG_i first verifies the message freshness by checking the validity of the time stamp. To verify the freshness, $NANG_i$ takes its current timestamp T_2 and checks whether $T_2 - T_1 \leq \delta T$ or not. Also, $NANG_i$ confirms that there were no other requests with parameters have been received between the time $(T_1 + \delta T)$ and $(T_1 - \delta T)$. If the timestamp T_1 is not modified in the login request message, the condition $T_2 - T_1 \leq \delta T$ will definitely fails and $NANG_i$ drops the session. This procedure also happens when SG_i receives login request message from $NANG_i$. Therefore, the proposed scheme resists the replay attack.

Resiliency against insider attack

The proposed distributed multistage authentication scheme does not store all the information in a single system/server. The registration of SM_i is with $NANG_i$ and the registration of $NANG_i$ will be done by SG_i. This process distributes the necessary credentials to SM_i, $NANG_i$ and SG_i. To perform any attack, insider must know parameters stored in other two participants SM_i and $NANG_i$. Hence the proposed scheme ensures resiliency against insider attack.

Resiliency against impersonation attack

When the communication has taken place in an open channel, the attacker can intercept the sent/received messages and perform an impersonation attack. Assume that an attacker $\mathscr{A}$ intercepts the login and authentication messages $\{C_{sm}, CID_i, C_1, T_1\}$, $\{CID_i, C_2, C_{nan}, RID_s, T_2, T_1\}$, $\{C_3, C_s, T_3\}$, and $\{C_s, T_3, C_4, C_m, T_4, RID_m\}$ to perform impersonation attack. In the proposed scheme, computation of the communication parameters are depending upon the random nonces w, y and the parameters $\{NID_i, b_j, V_n\}$ stored in SM_i. Since the random nonce and stored parameters do not communicate in the open channel as plain text, attacker $\mathscr{A}$ cannot get the knowledge of it. Therefore $\mathscr{A}$ cannot modify the login request parameters to impersonate the user.

Resiliency against man-in-the-middle attack

A man-in-the-middle attack can be possible when the adversary successfully authenticates with the server or calculate the session key correctly by intercepting communication messages. In the proposed scheme, to mitigate this attack we have applied two types of mechanism. First and foremost the communication message parameters of the proposed scheme are computed depending upon the generated random nonces w, y. Usage of random nonce prevents the impersonation and preserves the secrecy of the session key. Secondly, a timestamp has been used to check the validity of the login request message in every session. As said in "Resiliency Against Replay Attack", checking the message freshness resists the replay attack. Hence, the attacker cannot authenticate himself by intercepting the communication messages.

Provides perfect forward secrecy

In the proposed scheme, session key calculated by $SK = h_2(y.P_{pub} || w.P_{pub} || b_i || b_j)$. An adversary $\mathscr{A}$ cannot compute SK by intercepting the mutual authentication messages $\{C_3, C_s, T_3\}$, and $\{C_s, T_3, C_4, C_m, T_4, RID_m\}$. An attacker must have the knowledge of random nonces w, y, b_i and b_j to calculate SK. The proposed scheme cannot share random nonce as plain text over the public channel. Therefore to calculate SK, an adversary has to guess all random nonces at the same time, which is not possible. Hence the proposed scheme provides perfect forward secrecy.

Provides device anonymity

In the proposed scheme, device anonymity is preserved while login into the system. A dynamic identity $CID_i = h_1(w.P_{pub} || T_1) \oplus b_i$ has been calculated every session. The computation of the CID_i is depending on the random nonce w. Therefore the dynamic identity is different at every login attempt. Hence the proposed scheme provides reveal the device identity MID_i.

Provides data confidentiality

In the proposed scheme, the confidentiality of the communicated messages has been preserved even after authentication. The secrecy of the message after authentication can be achieved by the session key. In the proposed scheme, if the attacker tries to steal any message communicated between SM_i, $NANG_i$ and SG_i cannot decrypt without SK. As explained in "Provides Perfect Forward Secrecy", the session key cannot be compromised with the adversary. Moreover, during authentication, after successful verification of the login request SM_i, $NANG_i$ and SG_i will mutually authenticate each other and compute the session key. This creates a secure channel over an insecure environment. So, the communicated message remains confidential between SM_i, $NANG_i$ and SG_i.

From the cryptanalysis result of the proposed scheme it can be proved that the data confidentiality, sensitivity and the security has been achieved by resisting the possible attacks on the network.

FORMAL SECURITY PROOF

This section presents the formal security analysis to prove that the proposed scheme is secure against the adversary modeled in *Odelu et al. (2016)* and *Tsai & Lo (2015)* proposed by *Canetti & Krawczyk (2001)*. According to this mode, adversary $\mathscr{A}$ has full control over the transmission channel. Therefore $\mathscr{A}$ can eavesdrop, intercept, alter the communication messages, and knows all the public parameters. The adversary cannot access the secret parameter directly but can construct queries to capture the information leakage.

Participants

A participant in the entity takes part in the authentication process. In the proposed scheme, there are three participants are involved in performing the authentication, which is named as SM_i, $NANG_i$, and SG_i, where SM_i is a smart meter, $NANG_i$ for the Neighborhood Area Network gateway, and SG_i is the SCADA control center/Server. Each participant have multiple instances to run the scheme parallelly. The instances are represented as SM^i, $NANG^i$, and SG^i, where 'i' represents the ith instance of the participants (*Tsai & Lo, 2015*).

Queries

In CK—model, adversary $\mathscr{A}$ can construct the queries to perform the attacks. The possible queries made by $\mathscr{A}$, and the attacks committed with the constructed query are illustrated below:

- *Execute*(SM^i, $NANG^i$, SG^i): This oracle query construct the passive attacks by eavesdropping the successful execution done between the participants SM_i, $NANG_i$, SG_i. Here, $\mathscr{A}$ simulates the login and authentication phase and gets the messages communicated between the participants.
- *Send*($SM^i/NANG^i/SG^i$, M): $\mathscr{A}$ formulatess this query to perform active attacks. Adversary sends message to $SM^i/NANG^i/SG^i$ and receives the response from $SM^i/NANG^i/SG^i$. Also, $\mathscr{A}$ can intercept communication channel and modify the communicated messages and gets the reply in return.
- *EKeyReveal* (SM^i/SG^i): This query allows adversary to obtain the session state ephemeral secret key information held by the instance $SM^i/NANG^i/SG^i$.
- *SKReveal* (SM^i/SG^i): This query allows adversary to get the session key held by the instance $SM^i/NANG^i/SG^i$.
- *Corrupt* (SM^i/SG^i): This query express the notion of perfect forward secrecy where long term secret key can be compromise with $\mathscr{A}$ to get the session key on the oracle $SM^i/NANG^i/SG^i$.
- *Test*(SM^i/SG^i): This single query can be constructed by adversary at most once. It models the semantic security of the session. Here, $\mathscr{A}$ returns the session key of $SM^i/NANG^i/SG^i$ or a random string with an equal bit length of the session key. This result is depending upon tossing a coin b. If $b = 1$, the adversary gets the original session key. Else $\mathscr{A}$ gets a random string with the same length as the real session key.

 Before presenting the security proof, it is necessary to describe some definitions, which are given below:

- Partnering: Two entities are called to be partners when they are accepted and shared a commen session key. In the proposed scheme, SM_i, $NANG_i$ and SG_i are partners only if $MID_i = NID_j = SID_k$, and $SK_{SMi} = SK_{NANGi} = SK_{SGi}$.
- Freshness: It is related to the session key. Here, oracle constructs the session key. We can say that the constructed session key is fresh if the instance meets the following conditions.

1. When there is no *Reveal* query is done by SM_i, $NANG_i$ and SG_i, sission key SK_i should not be null.
2. $Send(SM_i, M)$, $Send(NANG_i, M)$ or $Send(SG_i, M)$ should be asked after modelling the *Currupt* query

- Semantic Security: The goal of semantic security is to guess the bit $'b'$, which is involved in the $Test(SM^i/SG^i)$ query. Consider an event $S()$ that the adversary $\mathscr{A}$ guess the bit b correctly. Let SM_i, $NANG_i$ and SG_i oracles are considered as partners when authenticating each other and share a common session key. The adversary's goal is to differentiate the session key from a random key. $\mathscr{A}$ can model many Test queries for SM^i or SG^i. Consider queries, for instance, SM^i. Further, SM^i toss a coin b. If b=1, the adversary gets the original session key. Else A gets a random string with the same length as the real session key.

 Let $Pr[S]$ denotes the game-winning probability of $\mathscr{A}$. The advantage of the Adversary A against breaking the semantic security of the proposed scheme is $Adv^{AKE}_P(A) = |2Pr[Succ] - 1|$.

Computational problem

It is essential to describe the details of the computational problem where the security proof relies upon.

- Elliptic curve computational Diffie-Hellman problem (ECDH): Let P, xP, $yP \in E_p$ where $a, b \in Z_q^*$, then it is hard to compute xyP in polynomial time without knowledge of x or y.
- Elliptic curve discrete logarithm problem (ECDLP): It says that when $G \in E_p(x, y)$ of order n and $G = kP \in E_p(x, y)$, it is computationally infeasible to compute k in polynomial-time.
- Reversing One way Hash function: Let $H(.)$ is a one way hash function, then it is computationally hard to get x from $H(x)$. Also it is hard to find x where $H(x) = H(x)$.

Security proof

Theorem 1 *Let E_p over the finite field F_p with a large prime number p and $\mathscr{D}$ be the finite set of password. Consider $\mathscr{A}$ is a adversary running in a polynomial time to perfom security*

Table 5 Simulation of send query.

For a hash oracle $h(i, q)$ where $i = 0, 1, 2$ if $(i, q, h) \in L_h$ Return h

Else, Choose h and add to L_h as (i, q, h)

For *Execute* $(SM^i, NANG^i, SG^i)$ query

$(CID_i, C_2, C_{nan}, RID_s, T_2, T_1) \leftarrow Send(C_{sm}, CID_i, C_1, T_1)$

$(C_3, C_s, T_3) \leftarrow Send(CID_i, C_2, C_{nan}, RID_s, T_2, T_1)$

$(C_s, T_3, C_4, C_m, T_4, RID_m) \leftarrow Send(C_3, C_s, T_3)$

Return $(C_{sm}, CID_i, C_1, T_1), (CID_i, C_2, C_{nan}, RID_s, T_2, T_1), (C_3, C_s, T_3), (C_s, T_3, C_4, C_m, T_4, RID_m)$

For *EKeyReveal* (SM^i/SG^i) query return Ephermal Secret key w from SM^i and y from SG^i

For *SKReveal* (SM^i/SG^i) query return static private key s from SM^i or SG^i

For *Test*$(SM^i/NANG^i/SG^i)$ query

$SK_p \leftarrow Revel(SM^i/NANG^i/SG^i)$

$b \leftarrow \{0, 1\}$

$SK_p \leftarrow \{0, 1\}^{k'}$

For *Corrupt*() query

If $P = P_i$

Return RPW_i or A_i

Else if $P = S$

Return A_i

attack on the proposed scheme. Let $Adv^{AKE}{}_{SC}$ is the advantage of the $\mathscr{A}$ against the proposed scheme and advantage of $\mathscr{A}$ that solves ECDH in E_p. While performing the attackes over the proposed scheme $\mathscr{A}$ makes q_{send} Send queries, q_{hsh} hash oracles, and q_{exe} Execute queries within the time t. The advantage of $\mathscr{A}$ will be

$$Adv^{SG}_{AKE} \leq \frac{(q_{send} + q_{exe})^2}{2n} + \frac{(q_{hsh})^2}{2^k} + \frac{q_{send}}{2^k + n} + q_{hsh}.Adv^{ECDH}_{EC}(t + (q_{exe} + q_{send})T_{EC})$$

Proof: The queries constructed by $\mathscr{A}$ has been presented in Tables 5 and 6. Based on the queries build by $\mathscr{A}$, the proof is presented. The sequence of experiments from *Experiment*$_0$ to *Experiment*$_4$ defines the proof of the proposed authenticaion scheme. Let $Succ_n$ denotes the event that occures after the *Test* query made by adversary while guessing the bit b correctly.

Experiment 0: This experiment corresponds to the real experiment in the random oracle model. By the definition, we have

$$Adv^{SG}_{AKE} \leq 2Pr[Succ_0] - 1$$

Experiment 1: This experiment simulates H_0, H_1, H_2 by maintaining two hash list L_h and L_h. Here, L_h stores the oracle for H_0, H_1, H_2 and L_h is for queries asked by $\mathscr{A}$. The simulation queries are presented in Table 5. From the simulation, it is observed that

Table 6 Simulation of execute, revel and test query.

For *Send* $(P^i, Start)$ query

Generate random number w and computes $C_{sm} = w.P_{pub} \oplus h_0(V_m || MID_i)$, $CID_i = h_1(w.P_{pub} || T_1) \oplus b_i$, $C_1 = h_1(CID_i || b_i || w.P_{pub})$, Return $(C_{sm}, CID_i, C_1, T_1)$.

For *Send* $(C_{sm}, CID_i, C_1, T_1)$ query

$w.P_{pub} = C_{sm} \oplus H_m$, $bi' = h_1(w.P_{pub} || T_1) \oplus CID_i$ $C_{nan} = C_{sm} \oplus H_m \oplus h_0(V_n || NID_i)$

$RID_s = h_1(C_{nan} || h_0(V_n || NID_i)) \oplus b_j$ $C_2 = h_1(C_1 || T_2 || C_{nan} || b_j)$ Return $(CID_i, C_2, C_{nan}, RID_s, T_2, T_1)$

For *Send* $(CID_i, C_2, C_{nan}, RID_s, T_2, T_1)$ query

$w.P_{pub'} = C_{nan} \oplus H_n$ $b_{i'} = h_1(w.P_{pub} || T_1) \oplus CID_i$ $b_j = h_1(C_n || H_n) \oplus RID_s$

$C_{1'} = h_1(CID_i || b_{i'} || w.P_{pub})$ $C_{2'} = h_1(C1' || T_2 || C_{nan} || b_j)$

If $C_{2'} = C_2$

Generate random number y and computes

$C_s = y.P_{pub} \oplus h_2(H_n)$ $SK_s = h_2(y.P_{pub} || w.P_{pub'} || b_i' || b_{j'})$ $C_3 = h_2(SK_s\ t_3\ y.P_{pub})$

Return (C_3, C_s, T_3)

For *Send* (C_3, C_s, T_3) query

$y.P_{pub} = C_s \oplus h_2(h_0(V_n || NID_i))$ $RID_m = h_2(C_m || H_m) \oplus b_j$ $C_m = C_s \oplus H_m \oplus h_2(h_0(V_n || NID_i))$

$SK_N = h_2(y.P_{pub} || w.P_{pub'} || b_i' || b_{j'})$ $C_4 = h_2(C_3 || T_4 || C_m || b_j)$

Return $(C_s, T_3, C_4, C_m, T_4, RID_m)$

For *Send* (C_3, C_s, T_3) query

$y.P_{pub'} = C_s \oplus h_0(V_m || MID_i)$ $b_{j'} = h_1(C_m || h_0(V_m || MID_i)) \oplus RID_m$ $SK_M = h_2(y.P_{pub'} || w.P_{pub} || b_i || b_{j'})$

$C_{3'} = h_2(SK_M || T_3 || y.P_{pub'})$ $C4' = h_2(C_{3'} || T_4 || C_m || b_j)$

If $C_4 = C_4$ SM_i, $NANG_i$ and SG_i Else Terminated

the transcript distribution of *Experiment* 0 and *Experiment* 1 are indistinguishable. Hence we have

$$Pr[Succ_0] = Pr[Succ_1]$$

Experiment 2: This experiment simulates the oracle of *Experiment* 1 except the collisions occurs in the transcripts and hash queries by the adversary. In other words, the experiment aims to avoid the collision occurring in C_1, C_3, C_{sm} and C_s. The *Experiment* 1 and *Experiment* 2 are indistinguishable until the collision takes place. Since, w and y are randomly chosen, according to the birthday paradox, probability of the collision occurrence is at most $(q_{send} + q_{exe})^2/2n$. Also, the probability of the occurrence of the collision in the output of the hash oracle is at most $(q_{hsh})^2/2^k$. Hence we have

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{(q_{send} + q_{exe})^2}{2n} + \frac{(q_{hsh})^2}{2^k} \qquad (1)$$

Experiment 3: This experiment aborts the scheme if the adversary succeeds in guessing the authentication value C_1 and C_3 without making the hash query. Since, *Experiment* 3 and *Experiment* 2 are indistinguishable unless smart grid SG_i rejects C_1 or smart meter SM_i rejects the authentic value C_3. Hence we have

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{q_{send}}{2^k + n} \qquad (2)$$

Experiment 4: This experiment considers the session key security. $\mathscr{A}$ cannot obtain the previous session key when $\mathscr{A}$ has $\{w, y, s, P\}$ but not (w, s, P) and (y, s, P). The aim of $\mathscr{A}$ is to compute the session key $SK_i = h_2(y.s.P \; w.s.P \; b_i \; b_j)$ by asking $Execute(SM^i, NANG^i, SG^i)$ queries and corresponding hash queries in the four cases.

case 1: $\mathscr{A}$ queries $Corrupt$ (SM^i) and $Corrupt$ (SG^i) to get static private key s to compute the session key SK_i. To derive the session key $\mathscr{A}$ should get w and y.

case 2: $\mathscr{A}$ queries $EKeyReveal$ (SM^i) and $EKeyReveal$ (SG^i) to get ephermal private key w and y. But $\mathscr{A}$ will not get the static key s.

case 3: $\mathscr{A}$ queries $EKeyReveal$ (SM^i) and $Corrupt$ (SG^i) and returns w and s. But $\mathscr{A}$ will not get y.

case 4: $\mathscr{A}$ queries $Corrupt$ (SM^i) and $EKeyReveal$ (SG^i) and returns y and s. But $\mathscr{A}$ will not get x.

In all the above four cases, $\mathscr{A}$ will get insufficient information to compute SK_i without solving the ECDH. The *Experiment* 3 and *Experiment* 4 are indistinguishable until the ECDH assumption is true. Hence we have

$$|Pr[Succ_4] - Pr[Succ_3]| = q_{hsh}.Adv_{EC}^{ECDH}(t + (q_{exe} + q_{send})T_{EC}) \qquad (3)$$

Now, $\mathscr{A}$ has to guess b to achieve the experiment by the *Test* query. It is clear that $Pr[Succ_4] = 1/2$.

RESULT OF FORMAL SECURITY VERIFICATION USING AVISPA TOOL

The results of the security verification using the AVISPA tool are presented in this section. AVISPA is a protocol analysis tool that provides a platform to implement the schemes and verify its security. To implement schemes, AVISPA uses High-Level Protocol Specification Language (HLPSL). It is a role-based language where every participant in the network plays a role during the execution. In HLPSL, the Doley-Yao model has been used to build the intruder. During the execution of schemes, the HLPSL code is converted into an Intermediate Format (IF) through a translator called hlpsl2if. Further, the translated IF is read by backends and analyses security goals. There are four backends are used in AVISPA used for security analysis known as On-the-fly Model-Checker (OFMC) (*Basin, Mödersheim & Vigano, 2005*), CL-AtSe (Constraint Logic-based Attack Searcher) (*Turuani, 2006*), SAT-based Model checker (*Armando & Compagna, 2004*) and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL

C:\progra~1\SPAN\testsuite\results\smart
_grid_improved.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.79s
  visitedNodes: 64 nodes
  depth: 6 plies
```

Figure 2 OFMC simulation result of proposed scheme.

(TA4SP) (*Boichut et al., 2004*). If the scheme achieves all defined goals, then the output is given as SAFE else, the output will be UNSAFE.

The results of the security verification obtained from the AVISPA tool are presented in Figs. 2 and 3. The presented results are obtained through OFMC, and CLAtSe back ends. The other two backends SATMC and TA4SP, do not support the XOR feature. Hence the results were received as "Inconclusive". Therefore the OFMC and CLAtSe results are considered and claimed that the obtained result is SAFE against the intruder. Hence, we can clearly say that the proposed scheme achieves all the specified goals and remains secure against all the attacks.

EFFICIENCY ANALYSIS

This section focuses on the efficiency analysis of the proposed scheme. The analysis mainly focuses on calculating the computation and communication costs and comparing the result with related authentication schemes like *Tsai & Lo (2015)*, *Wazid et al. (2017)*, *Odelu et al. (2016)*, *Gope & Sikdar (2018)*, *Kumar et al. (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)*, *Wu et al. (2019)*, *Li et al. (2019)* and *Khan, Kumar & Ahmad (2019)*.

Computation cost analysis

The proposed scheme's computation cost has been calculated and compared with the other schemes. We have presented the required computation cost and estimated execution time of the proposed scheme in Smart meter, NAN gateway, and SCADA control center/Server. To measure the execution time, we have taken the results obtained by *Gope & Sikdar (2018)*. According to the results presented by *Gope & Sikdar (2018)*, the required execution time for one computational parameter on Smart meter, NAN gateway, and SCADA control center/Server is given in Table 7. The computational parameters are

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL

C:\progra~1\SPAN\testsuite\results\smart_grid_impr
oved.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.18 seconds
  Computation: 0.00 seconds
```

Figure 3 CLAtSe simulation result of proposed scheme.

Table 7 Execution time of cryptographic operations.

Operation	SM_i & $NANG_i$	SG_i
T_h	0.026 ms	0.011 ms
T_s	0.079 ms	0.041 ms
T_{mp}	5.9 ms	2.6 ms
T_e	7.86 ms	2.34 ms
T_b	9.23 ms	3.78 ms
T_{PUF}	0.12 ms	–
T_{fe}	3.28 ms	1.17 ms

defined as follows: T_h: The time for executing a one-way hash operation, T_s: The time for symmetric key encryption/decryption execution operation, T_{mp}: scalar multiplication operation of an elliptic curve, T_a: Point addition operation of an elliptic curve, T_b: The time to perform one bilinear pairing operation, T_e: The time to complete the modular exponential operation, T_{fe}: The time to perform fuzzy extractor Gen(·)/Rep(·) operation, T_{PUF}: The time to perform Operation of PUF circuit.

The computation cost analysis results are given in the Table 8 and the estimated execution time analysis is presented Fig. 4. The computation cost of the proposed scheme is the sum of the costs of SM_i, $NANG_i$, and SG_i, which is $2T_{mp} + 12T_h$, $1T_{mp} + 12T_h$, and $1T_{mp} + 7T_h$, respectively. The total computation cost of the proposed scheme is $4T_{mp} +$

Table 8 Computation cost analysis.

Schemes	SM_i	$NANG_i$	SG	Total	Expected time
Tsai & Lo (2015)	$4T_{mp} + T_e + T_h$	–	$2T_b + 3T_{mp} + 1T_e + 5T_h$	$2T_b + 4T_{mp} + 2T_e + 6T_h$	49.421 ms
Wazid et al. (2017)	$4T_{mp} + 2T_{eca} + 5T_h$	–	$2T_{mp} + 1T_{fe} + 8T_h$	$6T_{mp} + 2T_{eca} + 1T_{fe} + 13T_h$	31.088 ms
Odelu et al. (2016)	$3T_{mp} + 1T_e + 6T_h$	–	$2T_{mp} + 2T_b + 1T_e + 6T_h$	$5T_{mp} + 2T_e + 1T_b + 12T_h$	40.882 ms
Gope & Sikdar (2018)	$1T_{fe} + 5T_h + 1T_{PUF}$	–	$1T_{fe} + 6T_h$	$2T_{fe} + 11T_h + 1T_{PUF}$	4.766 ms
Kumar et al. (2018)	$3T_{mp} + 2T_s + 4T_h$	$3T_{mp} + 2T_s + 5T_h$	–	$6T_{mp} + 4T_s + 9T_h$	35.875 ms
Zhang et al. (2019)	$1T_s + 7T_h$	–	$3T_s + 9T_h$	$4T_s + 16T_h$	0.483 ms
Ma et al. (2019)	$1T_{mp} + 2T_s + 7T_h$	–	$1T_{mp} + 4T_s + 14T_h$	$2T_{mp} + 6T_s + 21T_h$	9.158 ms
Wu et al. (2019)	$3T_e + T_{mp} + 4T_h$	$5T_e + T_{mp} + 4T_h$	–	$8T_e + 2T_{mp} + 8T_h$	74.888 ms
Li et al. (2019)	$2T_e + T_s + 4T_h$	$3T_e + T_{mp} + 4T_h$	–	$5T_e + T_s + T_{mp} + 4T_h$	46.198 ms
Khan, Kumar & Ahmad (2019)	$2T_{mp} + 1T_{fe} + 4T_h$	–	$2T_{mp} + 3T_h$	$4T_{mp} + 1T_{fe} + 7T_h$	20.417 ms
Proposed	$2T_{mp} + 12T_h$	$1T_{mp} + 12T_h$	$1T_{mp} + 7T_h$	$4T_{mp} + 31T_h$	21.001 ms
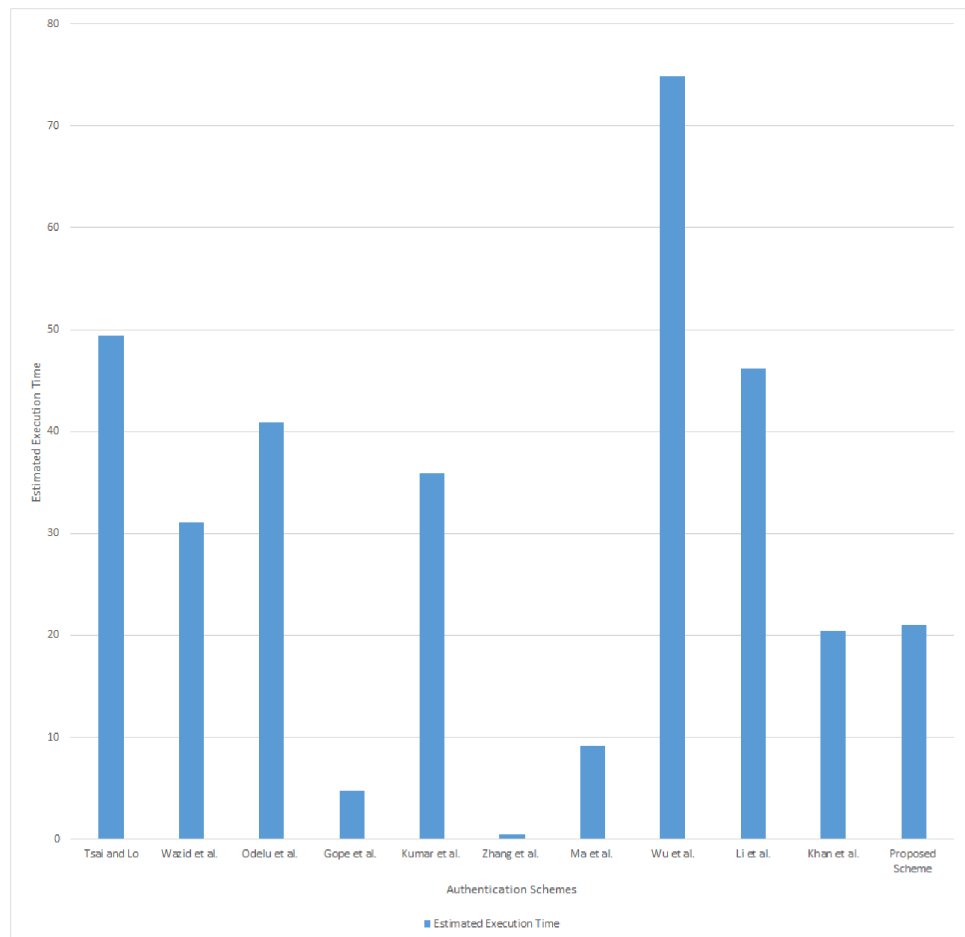
Figure 4 Computation cost analysis.

$32T_h$. Estimated execution time of the proposed scheme in the SM_i and $NANG_i$ is $(3 \times 5.9 \text{ ms}) + (24 \times 0.026 \text{ ms}) = 18.324 \text{ ms}$. The estimated execution time in the SG_i side is $(1 \times 2.6 \text{ ms}) + (7 \times 0.011 \text{ ms}) = 2.677 \text{ ms}$. The total estimated execution time of the proposed scheme is 21.001 ms.

Comparing the proposed scheme's results with the other schemes presented in Table 8, we can observe that the proposed scheme's computational cost and estimated execution time is higher than *Gope & Sikdar (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)*, *Khan, Kumar & Ahmad (2019)* schemes and lesser than all other schemes. Unlike the proposed scheme, *Gope & Sikdar (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)* schemes will not mutually authenticates every participants involved in the communication. There are some architectural limitations where the scheme can be applied only when the smart meter is directly communicates with the smart grid. As discussed in "Introduction", smart grid topology is split into several networks which contains several smart meters, NAN gateways, and SG. Therefore, the schemes of *Gope & Sikdar (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)* are not efficient for hierarchical model of smart grid communications. The estimated execution time of *Khan, Kumar & Ahmad's (2019)* scheme also less than the proposed scheme. But the khan2019elliptic scheme was limited to authenticate smart meters and NAN gateway only. The proposed scheme computation cost and estimated execution time include the mutual authentication of a smart meter, NAN gateway, and smart grid. Also, the authentication of the proposed scheme has been achieved without involvement of any third party. Therefore the computation cost looks higher than the schemes of *Gope & Sikdar (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)*, *Khan, Kumar & Ahmad (2019)*. However, the proposed scheme overcomes all the security barriers presented in "Functional Analysis", and achieves fully distributed multistage authentication.

Communication cost

The communication cost of the proposed scheme is compared with the *Tsai & Lo (2015)*, *Wazid et al. (2017)*, *Odelu et al. (2016)*, *Gope & Sikdar (2018)*, *Kumar et al. (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)*, *Wu et al. (2019)*, *Li et al. (2019)* and *Khan, Kumar & Ahmad (2019)* schemes and presented in Table 9. It includes the cost of the communication parameters, transmitted in one complete session of the authentication phase. For consistency purpose, we assume that the length of the identity ID_i and random number is 128 bits, the output size of hash functions H_0 (.), H_1 (), and H_2 () is 160 bits, size of an elliptic curve point is 320 bits, the block size of symmetric encryption/decryption is 256 bits, size of bilinear pairing is $G_1 \rightarrow 320$ bits, $G_2 \rightarrow 512$ bits and a Timestamp is 32 bits. The authentication phase of the proposed scheme requires $320 + 160 + 160 + 32 = 672$ bits, $160 + 160 + 160 + 160 + 32 + 32 = 704$ bits, $160 + 320 + 160 + 32 = 672$ bits, and $320 + 160 + 160 + 160 + 160 + 32 + 32 = 1074$ bits, for the messages $\{C_{sm}, CID_i, C_1, T_1\}$, $\{CID_i, C_2, C_{nan}, RID_s, T_1, T_2\}$, $\{C_3, C_s, T_3\}$, and $\{C_s, T_3, C_4, C_m, T_4, RID_m\}$. Hence, the total communication cost required for the proposed scheme to achieve the one session is 3072 bits. The communication cost analysis result is presented in Fig. 5.

We have also calculated the energy cost of the proposed scheme and compared the result with other schemes. The energy cost gives the expected energy required to
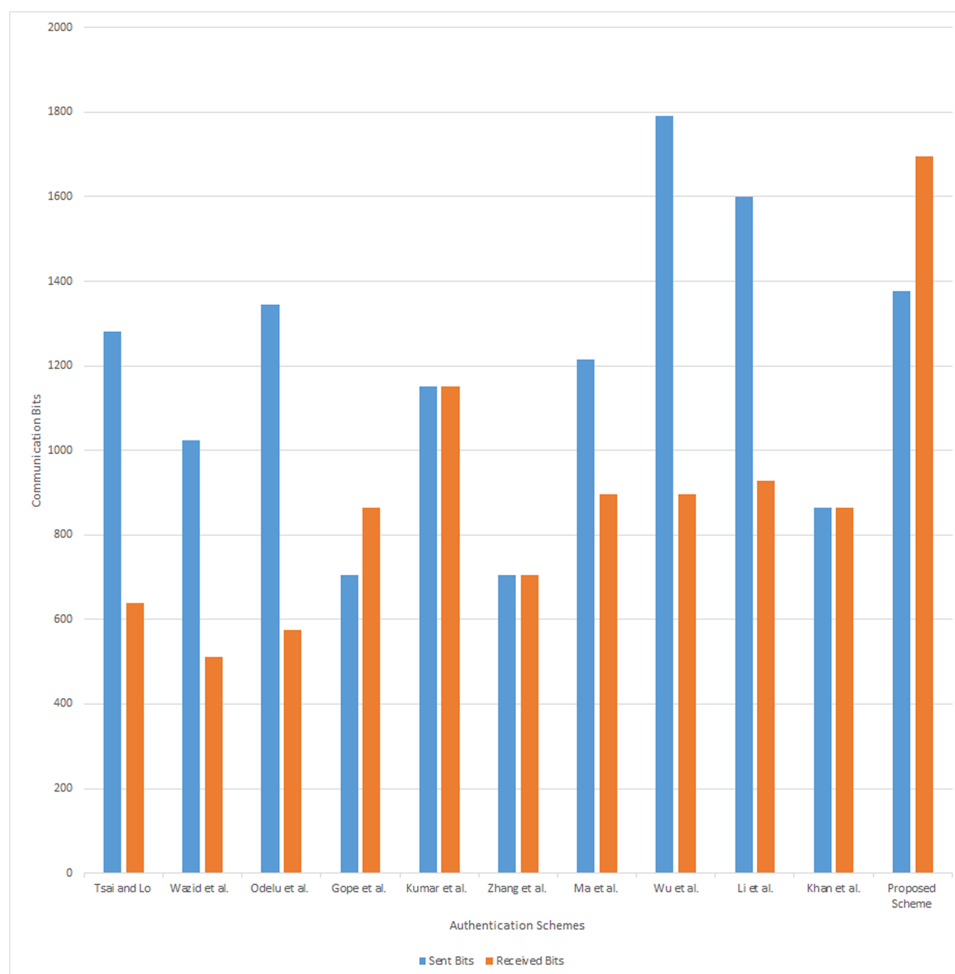
Figure 5 Communication analysis.

Table 9 Communication cost analysis.

Schemes	Send		Receive		Total	
	Comm. bits	Energy cost (μJ)	Comm. bits	Energy cost (μJ)	Comm. bits	Energy cost (μJ)
Tsai & Lo (2015)	1,280	921.6	640	518.4	1,920	1,440
Wazid et al. (2017)	1,024	737.28	512	414.72	1,536	1,152
Odelu et al. (2016)	1,344	967.68	576	466.56	1,920	1,434.24
Gope & Sikdar (2018)	704	506.88	864	699.84	1,568	1,206.72
Kumar et al. (2018)	1,152	829.44	1,152	933.12	2,304	1,762.56
Zhang et al. (2019)	704	506.88	704	570.24	1,408	1,077.12
Ma et al. (2019)	1,216	875.52	896	725.76	2,112	1,601.28
Wu et al. (2019)	1,792	1290.24	896	725.76	2,688	2,016
Li et al. (2019)	1,600	1152	928	751.68	2,528	1,903.68
Khan, Kumar & Ahmad (2019)	864	622.08	864	699.84	1,728	1,321.92
Proposed Scheme	1,376	990.72	1,696	1,373.76	3,072	2,364.48
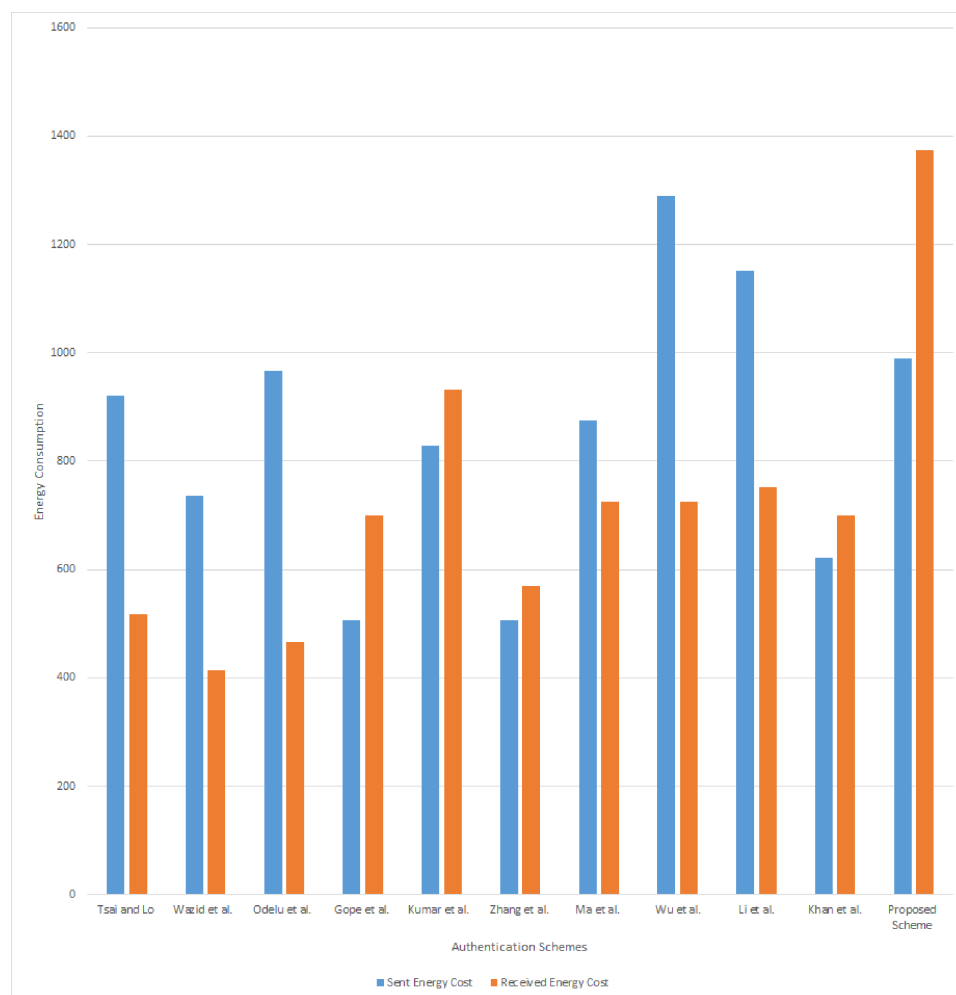
Figure 6 Energy consumption in communication.

communicate the data in the communication channel. We have used *De Meulenaer et al. (2008)* model to compute the energy cost. According to this model, the energy required to send and receive 1 bit of data is 0.72 μJ and 0.81 μJ, respectively. The communication cost of the sent message is 1,376 bits and received message is 1,696 bits, respectively. Hence, the energy cost of the proposed scheme for send and receive messages are 1,376 × 0.72 = 990.72 μJ and 1,696 × 0.81 = 1,373.76 μJ. The total expected energy cost of the proposed scheme is 2,364.48 μJ. The result of energy cost analysis has been presented in Table 9 and also shown in Fig. 6.

According to the analysis result presented in Table 9, the communication and energy costs of the proposed scheme are higher than all other schemes. Unlike other schemes the proposed scheme cost includes the communication done between smart meter, NAN gateway, and smart grid during the authentication. In Table 9, *Tsai & Lo (2015)*, *Wazid et al. (2017)*, *Odelu et al. (2016)*, *Gope & Sikdar (2018)*, *Zhang et al. (2019)*, *Ma et al. (2019)*, and *Khan, Kumar & Ahmad (2019)* schemes, have no communication with NAN gateway during authentication. Therefore, during communication cost comparison, if we

Table 10 Functional analysis.

Schemes	F1	F2	F3	F4	F5	F6	F7	F8	F9
Tsai & Lo (2015)	×	✓	×	×	✓	✓	✓	×	×
Wazid et al. (2017)	×	×	✓	×	✓	✓	✓	✓	✓
Odelu et al. (2016)	×	✓	×	✓	✓	✓	✓	✓	✓
Gope & Sikdar (2018)	×	✓	×	✓	✓	✓	×	✓	✓
Kumar et al. (2018)	×	✓	✓	✓	✓	✓	✓	×	✓
Zhang et al. (2019)	×	✓	×	×	✓	✓	✓	×	✓
Ma et al. (2019)	×	✓	×	✓	×	✓	✓	×	✓
Wu et al. (2019)	×	✓	✓	✓	✓	✓	✓	×	✓
Li et al. (2019)	×	✓	✓	✓	×	✓	✓	×	✓
Khan, Kumar & Ahmad (2019)	×	×	✓	✓	×	✓	✓	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓	✓	✓

neglect the proposed scheme communication messages done with NAN gateway, the total communication cost of the messages $\{C_{sm}, CID_i, C_1, T_1\}$, $\{C_3, C_s, T_3\}$ is 1,344 bits and the energy cost is 1,028.16 μJ which is less than other schemes. Similarly, *Kumar et al. (2018)*, *Wu et al. (2019)*, and *Li et al. (2019)* schemes have no communication between NAN gateway and smart grid, we neglect those communication done in the proposed scheme to do the comparison. Therefore the total communication cost of the messages $\{C_{sm}, CID_i, C_1, T_1\}$, $\{C_s, T_3, C_4, C_m, T_4, RID_m\}$ is 1,746 bits and the energy cost is 1,353.78 μJ which is lesser than other compared schemes. Hence, we claim that the proposed scheme is efficient than other schemes and robust in the multistage architecture.

Functional analysis

Table 10 presents the functional analysis of the proposed scheme done with other schemes. The features and the functionalities represented in Table 8 are as follows: F1—Multistage authentication, F2—Provide perfect forward secrecy, F3—Prevents replay attack, F4—Prevents insider attack, F5—Prevents man in middle attack, F6—Prevents impersonate attack, F7—Provide mutual authentication, F8— Provide smart meter credentials privacy, F9—Provides session key security. From Table 10, it is clear that the proposed scheme meets all the functional requirements. It also achieves multistage authentication where one smart grid can authenticate the smart meter through the NAN gateway.

CONCLUSIONS

The security of smart meter communication is critical for reliable, efficient and stable operation of a contemporary smart grid. This paper addresses the security issues by considering a novel authentication scheme for smart meter communication with the energy control center. The proposed method is based on a novel formulation, where the authentication scheme is dynamic, multi-stage and distributed in nature. The formal proves presented in this paper validate that the proposed model can establish a secure authentication path between a smart meter, NAN gateway, and a SCADA energy center in a distributed manner. We also verified the effectiveness of the proposed authentication

scheme against adversarial attacks using a simulation tool AVISPA. Considering the computation, communication and functional costs, this article also presented the efficiency analysis of the proposed authentication scheme. Based on comparative analyses, we can conclude that the proposed scheme is robust and secure as compared to the existing related schemes. Hence, the proposed authentication scheme has the potential to secure smart meter communication between the energy consumers and utility control centers to foster an attack resilient sustainable energy grid.

APPENDIX

The implementation of the proposed scheme in AVISPA includes the registration phase and the login and authentication phase. Here, three leading roles are named as meter, gateway, and server, represented as SM_i, $NANG_i$ and S_j. The role specification of the meter is presented in Fig. 7. Here, the process begins by receiving a start signal. The gateway and server roles implementations are given in Figs. 8 and 9. SM_i, $NANG_i$ and S_j use symmetric key SKuisj for the communication in the channel. The send and receive channels required for communication between meter, gateway, and server are represented by Snd() and Rcv() functions.

Figures 10 and 11 present the session and environment roles. The session role includes the primary roles for composition and the channels of all roles involved in communication. The environment role specifies the global constants and sessions for an adversary to play as legitimate user roles. It also defines the goals of the proposed scheme.

```
role meter (SMi, NANGi, Sj : agent,
      SKuisj : symmetric_key,
      Snd,RCV :channel(dy))
% Ui is the user; Sj is the server
played_by SMi
def=
 local State : nat,
      NIDi, MIDi, CIDi, RIDm, RIDs, Bj, Bi, Ai, Aj, Vn, Vm, Hn, Hm, Csm, Cs, Cm, C1, C2, C3, C4: text,
      T1, T2, T3, T4, W, Y, SKn, SKs, SKm, S, E, Qi, Qs: text,
      Ec, H0, H1, H2 : hash_func
      const subs1, subs2, subs3, smi_sj_w,smi_sj_T1, sj_smi_y, sj_smi_T2 : protocol_id
init State:=0
         transition
1.        State=0 /\ RCV(start)=|>
          State':=1 /\ Bi':=new()
          /\Aj' := H0(MIDi, Bi')
% Send the registration request message
          /\ Snd({MIDi.Aj}_SKuisj)
          /\ secret({MIDi, Bi}, subs1, {SMi, NANGi})
          /\ secret({Bi}, subs2, NANGi)
% Receive the request from the Smart meter SMi
 2. State = 1 /\RCV({Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi)))}_SKuisj) =|>

% Login phase
 State':= 2
              /\ W' := new()
              /\ T1' := new()
              /\ Qi' := Ec(W')
              /\ Csm' := xor(Qi', H0(Vm. MIDi))
              /\ CIDi' := xor(H1(Qi'. T1), Bi)
              /\ C1' := H1(CIDi', Bi, Qi')
              /\ Snd ({CIDi. T1. Csm. C1}_SKuisj)
              /\ secret({W}, subs3, {SMi, NANGi, Sj})
        /\ witness(SMi, Sj, smi_sj_w, W')
        /\ witness(SMi, Sj, smi_sj_T1, T1')

% Authentication phase
% Receive the authentication request message
3. State = 2 /\ RCV ({xor(Ec(Y'), H2(H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi))).T3.H2((H2(H2(Ec(Y'). Ec(W'). Bi. Bj). T3.
Ec(Y'))).T4.xor(xor((xor(Ec(Y'), H2(H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi)))),(H0((Ec(H0((H0((Ec((H0(s.e).
H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi)))).MIDi))), H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi)).Bj).xor(xor((xor(Qs',
H2(H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi))), (H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj)))). NIDi)).(H0(MIDi.Bi)))).
MIDi))), H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi)).T4.xor(H2(xor(xor((xor(Ec(Y'), H2(H0 (Ec(H0((H0(s.e)).(H0(NIDi.
Bj)))).NIDi)))), (H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi)))).MIDi))), H0((Ec(H0((H0(s.e)).
(H0(NIDi.Bj)))).NIDi)).(H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi)))).MIDi))), Bj)}_SKuisj) =|>

 State' := 3 /\ Qs' := xor((xor(Ec(Y'), H2(H0(Ec(H0((H0(s.e)). (H0(NIDi.Bj)))).NIDi)))), H0(Ec(H0((H0(s.e)).
(H0(NIDi.Bj)))).NIDi))
              /\ Cm' := xor(xor((xor(Qs', H2(H0((Ec(H0((H0(s.e)). (H0(NIDi.Bj)))).NIDi)))), (H0((Ec(H0((H0((Ec((H0(s.e).
H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi)))).MIDi))), H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi))
              /\RIDm' := xor(H2(Cm.(H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi)))).MIDi))), Bj)
              /\ Bj' := xor(H1(Cm'.H0(Ec(H0(H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi).Aj)).MIDi)), RIDm')
              /\ SKm' := H2(Qs'. Qs'.Bi'.Bj')
              /\ C3' := H2(SKm.T3'.Qs')
              /\ C4' := H2(C3'.T4.Cm.Bj)
          /\ request(SMi, Sj, sj_smi_y, Y')
          /\ request(SMi, Sj, sj_smi_T2, T2')
        end role
```

Figure 7 Role specification for the SMi of the proposed scheme.

```
role gateway (SMi, NANGi, Sj : agent,
      SKuisj : symmetric_key,
      Snd,RCV :channel(dy))
% Ui is the user; Sj is the server
played_by NANGi
def=
 local State : nat,
      NIDi, MIDi, CIDi, RIDm, RIDs, Bj, Bi, Ai, Aj, Vn, Vm, Hn, Hm, Csm, Cnan, Cs, Cm, C1, C2, C3, C4: text,
      T1, T2, T3, T4, W, Y, SKn, SKs, SKm, S, E, Qi, Qs: text,
      Ec, H0, H1, H2 : hash_func
      const subs1, subs2, subs3, smi_sj_w,smi_sj_T1, sj_smi_y, sj_smi_T2 : protocol_id

init State := 0
      transition
% Registration phase
% Receive the registration request message from the SMi

1.        State=0 /\ RCV(start)=|>
          State':=1 /\ Bj':=new()
          /\Ai' := H0(NIDi, Bj')
          /\ Snd({NIDi.Ai}_SKuisj)

2.     State=1 /\ RCV({Ec(H0((H0(s.e)).(H0(NIDi.Bj))))}_SKuisj)=|>
          State':=2 /\ secret({MIDi, Bi}, subs1, {SMi, NANGi})
                         /\ secret({Bi}, subs2, NANGi)

3.        State=2 /\ RCV({MIDi.H0(MIDi.Bi)}_SKuisj)=|>
          State':=3 /\Hn' := H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj)))))).NIDi)
                    /\Vm' := Ec(H0(Hn.Aj))
                    /\Hm' := H0(Vm.MIDi)
                    /\ Snd({Vm}_SKuisj)

4.        State=3 /\ RCV({xor(H1(Ec(W). T1), Bi). T1. xor(Ec(W), H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj))))).NIDi)).(H0
(MIDi.Bi))))).MIDi)). H1(xor(H1(Ec(W). T1), Bi). Bi. Ec(W))}_SKuisj)=|>
          State':=4 /\ Qi' := xor(xor(Ec(W'), H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi))))). MIDi)), (H0((Ec
(H0((H0((Ec((H0(s.e). H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi))))).MIDi)))
                    /\ Bi' := xor(H1(Qi'.T1), xor(H1(Qi'. T1), Bi'))
                    /\Cnan' := xor(xor((xor(Ec(W'), H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi))))). MIDi))),
H0((Ec(H0((H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi))) ).MIDi)), H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi))
                    /\RIDs' := xor(H1(Cnan.H0((Ec(H0((H0(s.e)). (H0(NIDi.Bj))))).NIDi)), Bj)
                    /\C2' := H1((H1((xor(H1(Qi'. T1), Bi)). Bi. Qi')).T2.Cnan.Bj)
                    /\ Snd ({CIDi.C2.Cnan.RIDs.T2.T1}_SKuisj)

5.        State = 4 /\ RCV({H2((H2(Ec(Y'). Ec(W'). Bi'. Bj')). t3. (Ec(Y'))).xor(Ec(Y'), H2(H0(Ec(H0((H0(s.e)). (H0(NIDi.Bj))))).
NIDi))).T3}_SKuisj) =|>
              State' := 5 /\ T4' := new()
              /\Qs' := xor((xor(Ec(Y'), H2(H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)))), H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).
NIDi))
              /\ Cm' := xor(xor((xor(Qs', H2(H0((Ec(H0((H0(s.e)). (H0(NIDi.Bj))))).NIDi)))), (H0((Ec(H0((H0((Ec((H0(s.e).
H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi))))).MIDi))), H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi))
              /\RIDm' := xor(H2(Cm.(H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi))))).MIDi))), Bj)
              /\SKn' := H2(Qs'. Qi'. Bi'. Bj')
              /\C4' := H2((H2(SKn. T3. Qs')).T4.Cm.Bj)
          /\ Snd({Cs.T3.C4.Cm.T4.RIDm}_SKuisj)
end role
```

Figure 8 Role specification for the NANGi of the proposed scheme.

```
role server (SMi, NANGi, Sj : agent,
      SKuisj : symmetric_key,
      Snd,RCV :channel(dy))
% Ui is the user; Sj is the server

played_by Sj
def=
 local State : nat,
      NIDi, MIDi, CIDi, RIDm, RIDs, Bj, Bi, Ai, Aj: text,
      Vn, Vm, Hn, Hm, Csm, Cnan, Mi, Cs, Cm, C1, C2, C3, C4: text,
      T1, T2, T3, W, Y, SKn, SKs, SKm, S, E, Qi, Qs: text,
      Ec, H0, H1, H2 : hash_func
      const subs1, subs2, subs3, smi_sj_w, smi_sj_T1, sj_smi_y, sj_smi_T2 : protocol_id
init State:=0
          transition
1.        State=0 /\ RCV({NIDi.H0(NIDi.Bj)}_SKuisj)=|>
          State':=1 /\ E':=new()
                        /\Mi' := H0(s.e)
                        /\Vn' := Ec(H0(Mi.(H0(NIDi.Bj))))
                        /\Hn' := H0(Vn.NIDi)
% Send the registration request message
          /\ Snd({Vn}_SKuisj)

% Receive the smart card from the registration server Sj
 2. State = 1 /\RCV({xor(H1(Ec(W'). T1), Bi).H1((H1((xor(H1(Ec(W'). T1), Bi)). Bi. Ec(W))).T2.xor(xor((xor(Ec(W'), H0((Ec(H0
((H0((Ec((H0(s.e).H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi))))). MIDi))), H0((Ec(H0((H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)).
(H0(MIDi.Bi)))) ).MIDi)), H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi)).Bj).xor(xor((xor(Ec(W'), H0((Ec(H0((H0((Ec((H0(s.e).
H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi))))). MIDi))), H0((Ec(H0((H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi)))) ).MIDi
)),H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi)).xor(H1(Cnan.H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)), Bj).T2.T1}_SKuisj) =|>

% Login phase
 State':= 2
          /\Cnan' := xor(xor((xor(Ec(W'), H0((Ec(H0((H0((Ec((H0(s.e).H0(NIDi.Bj)))).NIDi)).(H0(MIDi.Bi))))). MIDi))), H0((Ec
(H0((H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)).(H0(MIDi.Bi)))) ).MIDi)), H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi))
          /\Hn' := H0(Ec(H0((H0(s.e)).(H0(NIDi.Bj)))).NIDi)
          /\ Qi':=xor(Cnan, Hn)
            /\ Bi' := xor(H1(Qi'.T1), xor(H1(Qi'. T1), Bi))
            /\ Bj' := xor(H1(Cnan.Hn), (xor(H1(Cnan.H0((Ec(H0((H0(s.e)).(H0(NIDi.Bj))))).NIDi)), Bj)))
            /\ C1' := H1((xor(H1(Ec(W'). T1), Bi)).Bi'.Qi')
            /\C2' := H1(C1'.T2.Cnan.Bj')
%Mutual authentication begins
            /\ Y' := new()
            /\ Qs' := Ec(Y')
            /\Cs' := xor(Qs', H2(Hn))
            /\SKs' := H2(Qs'. Qi'. Bi'. Bj')
            /\C3' := H2(SKs'. T3. Qs')
          /\ Snd ({C3.Cs.T3}_SKuisj)
          /\ witness(SMi, Sj, sj_smi_y, Y')
          /\ witness(SMi, Sj, sj_smi_T2, T2')
% Ui has freshly generated the timestamp T1 for Sj
          /\ request(SMi, Sj, smi_sj_w, W')
          /\ request(SMi, Sj, smi_sj_T1, T1')
        end role
```

Figure 9 Role specification for the SGi of the proposed scheme.

```
role session(SMi, NANGi, Sj : agent,
    SKuisj : symmetric_key)
def=
local Send1, Send2, Send3, Recv1,
Recv2,Recv3: channel (dy)
composition
    meter(SMi, NANGi, Sj, SKuisj, Send1,
Recv1)
    /\gateway(SMi, NANGi, Sj, SKuisj, Send2,
Recv2)
    /\server(SMi, NANGi, Sj, SKuisj, Send3,
Recv3)
end role
```

Figure 10 Role specification for the session of the proposed scheme.

```
role environment()
def=
const smi, nangi, sj: agent,
skuisj : symmetric_key,
nidi, midi, cidi, ridm, rids, bj, bi, ai, aj:text,
vn, vm, hn, hm, csm, cs, cm, c1, c2, c3, c4, t1, t2, t3, t4: text,
w, y, skn, sks, skm, s, e, qi, qs: text,
ec, h0, h1, h2:hash_func,
subs1, subs2, subs3, smi_sj_w,smi_sj_T1, sj_smi_y, sj_smi_T2 :
protocol_id

intruder_knowledge = {smi, nangi, sj, ec, h0, h1, h2, c1, c2, c3, t1, t2, t3, t4,
cidi, ridm, rids}
composition
session(smi, nangi, sj, skuisj)
/\session(smi, nangi, sj, skuisj)
/\session(smi, nangi, sj, skuisj)
end role
goal
secrecy_of subs1, subs2, subs3
authentication_on smi_sj_w, smi_sj_T1, sj_smi_y, sj_smi_T2
end goal
environment()
```

Figure 11 Role specification for the goal and environment of the proposed scheme.

Funding

The authors received no funding for this work.

Competing Interests

The authors declare that they have no competing interests.

Author Contributions

- Manjunath Hegde performed the experiments, analyzed the data, performed the computation work, prepared figures and/or tables, and approved the final draft.
- Adnan Anwar performed the experiments, analyzed the data, prepared figures and/or tables, and approved the final draft.
- Karunakar Kotegar conceived and designed the experiments, authored or reviewed drafts of the paper, and approved the final draft.
- Zubair Baig conceived and designed the experiments, prepared figures and/or tables, and approved the final draft.
- Robin Doss conceived and designed the experiments, authored or reviewed drafts of the paper, and approved the final draft.

Data Availability

The code is available in the Supplemental Files.

Supplemental Information

Supplemental information for this article can be found online at http://dx.doi.org/10.7717/peerj-cs.643#supplemental-information.

REFERENCES

Abbasinezhad-Mood D, Nikooghadam M. 2018. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. *Future Generation Computer Systems* **84(2)**:47–57 DOI 10.1016/j.future.2018.02.034.

Abbasinezhad-Mood D, Ostad-Sharif A, Nikooghadam M. 2019. Novel chaotic map-based privacy-preserving authenticated key agreement scheme without the electricity service provider involvement. *Security and Privacy* **2(5)**:e74 DOI 10.1002/spy2.74.

Aghapour S, Kaveh M, Martn D, Mosavi MR. 2020. An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications. *IEEE Access* **8**:125477–125487 DOI 10.1109/ACCESS.2020.3007623.

Anwar A, Mahmood AN, Ahmed M. 2015. *False data injection attack targeting the LTC transformers to disrupt smart grid operation.* Berlin: Springer International Publishing, 252–266.

Anwar A, Mahmood AN, Pickering M. 2016. *Intelligence and security informatics, chapter data-driven stealthy injection attacks on smart grid with incomplete measurements.* Cham: LNCS, Springer, 180–192.

Anwar A, Mahmood AN, Pickering M. 2017. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. *Journal of Computer and System Sciences* **83(1)**:58–72 DOI 10.1016/j.jcss.2016.04.005.

Anwar A, Mahmood AN, Tari Z. 2015. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid. *Information Systems* **53(1)**:201–212 DOI 10.1016/j.is.2014.12.001.

Anwar A, Mahmood AN, Tari Z. 2017. Ensuring data integrity of OPF module and energy database by detecting changes in power flow patterns in smart grids. *IEEE Transactions on Industrial Informatics* **13(6)**:3299–3311 DOI 10.1109/TII.2017.2740324.

Armando A, Compagna L. 2004. Satmc: a sat-based model checker for security protocols. In: *European Workshop on Logics in Artificial Intelligence*. Springer, 730–733.

Aziz IT, Jin H, Abdulqadder IH, Alturfi SM, Alobaidi WH, Flaih FM. 2019. T2S2G: a novel two-tier secure smart grid architecture to protect network measurements. *Energies* **12(13)**:2555 DOI 10.3390/en12132555.

Basin D, Mödersheim S, Vigano L. 2005. OFMC: a symbolic model checker for security protocols. *International Journal of Information Security* **4(3)**:181–208 DOI 10.1007/s10207-004-0055-7.

Boichut Y, Héam P-C, Kouchnarenko O, Oehl F. 2004. Improvements on the genet and klay technique to automatically verify security protocols. In: *Proceedings AVIS*. Vol. 4.

Canetti R, Krawczyk H. 2001. Analysis of key-exchange protocols and their use for building secure channels. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 453–474.

Chen Y, Martnez J-F, Castillejo P, López L. 2019. A bilinear map pairing based authentication scheme for smart grid communications: Pauth. *IEEE Access* **7**:22633–22643 DOI 10.1109/ACCESS.2019.2898376.

De Meulenaer G, Gosset F, Standaert F-X, Pereira O. 2008. On the energy cost of communication and cryptography in wireless sensor networks. In: *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. Piscataway: IEEE, 580–585.

DELWP. 2020. Smart meters in victoria, australia. *Available at* https://www.energy.vic.gov.au/electricity/smart-meters.

Eder-Neuhauser P, Zseby T, Fabini J. 2016. Resilience and security: a qualitative survey of urban smart grid architectures. *IEEE Access* **4**:839–848 DOI 10.1109/ACCESS.2016.2531279.

Fouda MM, Fadlullah ZM, Kato N, Lu R, Shen X. 2011. Towards a light-weight message authentication mechanism tailored for smart grid communications. In: *2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. Piscataway: IEEE, 1018–1023.

Gope P, Sikdar B. 2018. Privacy-aware authenticated key agreement scheme for secure smart grid communication. *IEEE Transactions on Smart Grid* **10(4)**:3953–3962 DOI 10.1109/TSG.2018.2844403.

Hancock B. 2001. Security views. *Computers & Security* **20(5)**:348363.

Irshad A, Chaudhry SA, Alomari OA, Yahya K, Kumar N. 2020. A novel pairing-free lightweight authentication protocol for mobile cloud computing framework. Epub ahead of print 19 June 2020. *IEEE Systems Journal* DOI 10.1109/JSYST.2020.2998721.

Kaspersky ICS CERT. 2020. Threat landscape for industrial automation systems. Kaspersky ICS CERT Report. *Available at* https://ics-cert.kaspersky.com/reports/2020/09/24/threat-landscape-for-industrial-automation-systems-h1-2020/ (accessed 9 March 2021).

Khan AA, Kumar V, Ahmad M. 2019. An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach. Epub ahead of print 29 April

2019. *Journal of King Saud University-Computer and Information Sciences* DOI 10.1016/j.jksuci.2019.04.013.

Koblitz N. 1987. Elliptic curve cryptosystems. *Mathematics of Computation* **48(177)**:203–209 DOI 10.1090/S0025-5718-1987-0866109-5.

Kumar P, Gurtov A, Sain M, Martin A, Ha PH. 2018. Lightweight authentication and key agreement for smart metering in smart energy networks. *IEEE Transactions on Smart Grid* **10(4)**:4349–4359 DOI 10.1109/TSG.2018.2857558.

Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A. 2019. Smart grid metering networks: a survey on security, privacy and open research issues. *IEEE Communications Surveys & Tutorials* **21(3)**:2886–2927 DOI 10.1109/COMST.2019.2899354.

Li H, Lu R, Zhou L, Yang B, Shen X. 2013. An efficient merkle-tree-based authentication scheme for smart grid. *IEEE Systems Journal* **8(2)**:655–663 DOI 10.1109/JSYST.2013.2271537.

Li X, Wu F, Kumari S, Xu L, Sangaiah AK, Choo K-KR. 2019. A provably secure and anonymous message authentication scheme for smart grids. *Journal of Parallel and Distributed Computing* **132**:242–249 DOI 10.1016/j.jpdc.2017.11.008.

Li S, Xue K, Yang Q, Hong P. 2017. PPMA: privacy-preserving multisubset data aggregation in smart grid. *IEEE Transactions on Industrial Informatics* **14(2)**:462–471 DOI 10.1109/TII.2017.2721542.

Ma Z, Yang Y, Liu X, Liu Y, Ma S, Ren K, Yao C. 2019. Emir-auth: eye-movement and iris based portable remote authentication for smart grid. *IEEE Transactions on Industrial Informatics* **16(10)**:6597–6606.

Mahmood K, Chaudhry SA, Naqvi H, Kumari S, Li X, Sangaiah AK. 2018. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems* **81(2)**:557–565 DOI 10.1016/j.future.2017.05.002.

Mahmood K, Chaudhry SA, Naqvi H, Shon T, Ahmad HF. 2016. A lightweight message authentication scheme for smart grid communications in power sector. *Computers & Electrical Engineering* **52(4)**:114–124 DOI 10.1016/j.compeleceng.2016.02.017.

Moghadam MF, Nikooghadam M, Mohajerzadeh AH, Movali B. 2020. A lightweight key management protocol for secure communication in smart grids. *Electric Power Systems Research* **178(8)**:106024 DOI 10.1016/j.epsr.2019.106024.

Ni Z, Paul S. 2019. A multistage game in smart grid security: a reinforcement learning solution. *IEEE Transactions on Neural Networks and Learning Systems* **30(9)**:2684–2695 DOI 10.1109/TNNLS.2018.2885530.

Nicanfar H, Jokar P, Beznosov K, Leung VC. 2013. Efficient authentication and key management mechanisms for smart grid communications. *IEEE Systems Journal* **8(2)**:629–640 DOI 10.1109/JSYST.2013.2260942.

Odelu V, Das AK, Kumari S, Huang X, Wazid M. 2017. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. *Future Generation Computer Systems* **68(1)**:74–88 DOI 10.1016/j.future.2016.09.009.

Odelu V, Das AK, Wazid M, Conti M. 2016. Provably secure authenticated key agreement scheme for smart grid. *IEEE Transactions on Smart Grid* **9(3)**:1900–1910 DOI 10.1109/TSG.2016.2602282.

Sadhukhan D, Ray S, Obaidat MS, Dasgupta M. 2020. A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. *Journal of Systems Architecture* **114**:101938.

Shin D, He S, Zhang J. 2014. Robust and cost-effective architecture design for smart grid communications: a multi-stage middleware deployment approach. In: *IEEE INFOCOM, 2014—IEEE Conference on Computer Communications.* Piscataway: IEEE, 2822–2830.

Tsai J-L, Lo N-W. 2015. Secure anonymous key distribution scheme for smart grid. *IEEE Transactions on Smart Grid* 7(2):906–914 DOI 10.1109/TSG.2015.2440658.

Turuani M. 2006. The cl-atse protocol analyser. In: *International Conference on Rewriting Techniques and Applications.* Springer, 277–286.

Wang W, Lu Z. 2013. Cyber security in the smart grid: survey and challenges. *Computer Networks* 57(5):1344–1371 DOI 10.1016/j.comnet.2012.12.017.

Wazid M, Das AK, Kumar N, Rodrigues JJ. 2017. Secure three-factor user authentication scheme for renewable-energy-based smart grid environment. *IEEE Transactions on Industrial Informatics* 13(6):3144–3153 DOI 10.1109/TII.2017.2732999.

Wu T-Y, Lee Y-Q, Chen C-M, Tian Y, Al-Nabhan NA. 2021. An enhanced pairing-based authentication scheme for smart grid communications. *Journal of Ambient Intelligence and Humanized Computing* 2021:1–13.

Wu L, Wang J, Zeadally S, He D. 2019. Anonymous and efficient message authentication scheme for smart grid. *Security and Communication Networks* 2019(4):1–12 DOI 10.1155/2019/4836016.

Wu D, Zhou C. 2011. Fault-tolerant and scalable key management for smart grid. *IEEE Transactions on Smart Grid* 2(2):375–381 DOI 10.1109/TSG.2011.2120634.

Xia J, Wang Y. 2012. Secure key distribution for the smart grid. *IEEE Transactions on Smart Grid* 3(3):1437–1443 DOI 10.1109/TSG.2012.2199141.

Yang Q, Yang J, Yu W, An D, Zhang N, Zhao W. 2014. On false data-injection attacks against power system state estimation: modeling and countermeasures. *IEEE Transactions on Parallel and Distributed Systems* 25(3):717–729 DOI 10.1109/TPDS.2013.92.

Zhang L, Zhao L, Yin S, Chi C-H, Liu R, Zhang Y. 2019. A lightweight authentication scheme with privacy protection for smart grid communications. *Future Generation Computer Systems* 100(9):770–778 DOI 10.1016/j.future.2019.05.069.

Zhong J, Chim T, Hui C. 2015. PRGA: privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Transactions on Dependable and Secure Computing* 12(1):85–97 DOI 10.1109/TDSC.2014.2313861.