LAS-SG: An Elliptic Curve-Based Lightweight Authentication Scheme for Smart Grid Environments

Shehzad Ashraf Chaudhry, Khalid Yahya, Sahil Garg, *Member, IEEE*, Georges Kaddoum, Mohammad Mehedi Hassan, *Senior Member, IEEE*, and Yousaf Bin Zikria, *Senior Member, IEEE*

***Abstract*—The communication among smart meters (SMs) and neighborhood area network (NAN) gateways is a fundamental requisite for managing the energy consumption at the consumer site. The bidirectional communication among SMs and NANs over the insecure public channel is vulnerable to impersonation, SM traceability, and SM physical capturing attacks. Many existing schemes' insecurities and/or inefficiencies call for an efficient and secure authentication scheme for smart grid infrastructure. In this article, we present a privacy preserving and lightweight authentication scheme for smart grid (LAS-SG) using elliptic curve cryptography. The proposed *LAS-SG* is proved as secure under the standard model. Moreover, the efficiency of the LAS-SG is extracted through a real-time experiment, which attests that proposed *LAS-SG* completes a round of authentication in 20.331 ms by exchanging only two messages and 192 B. Due to the adequate efficiency and ample security, the proposed *LAS-SG* is more appropriate for SG environments.**

***Index Terms*—Key compromise impersonation (KCI) attack, smart grid authentication, smart home.**

Manuscript received 15 December 2021; revised 30 January 2022; accepted 4 March 2022. Date of publication 15 March 2022; date of current version 13 December 2022. This work was supported by the King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP 2022/18. Paper no. TII-21-5569. *(Corresponding author: Yousaf Bin Zikria.)*

Shehzad Ashraf Chaudhry is with the Department of Computer Engineering, Faculty of Engineering and Architecture, Nisantasi University, 34398 Istanbul, Turkey, and also with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates (e-mail: ashraf.shehzad.ch@gmail.com).

Khalid Yahya is with the Department of Mechatronics Engineering, Istanbul Gelisim University, 34310 Istanbul, Turkey (e-mail: koyahya@gelisim.edu.tr).

Sahil Garg and Georges Kaddoum are with the Electrical Engineering Department, École de technologie supérieure, Montréal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org; georges.kaddoum@etsmtl.ca).

Mohammad Mehedi Hassan is with the Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mmhassan@ksu.edu.sa).

Yousaf Bin Zikria is with the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea (e-mail: yousafbinzikria@ynu.ac.kr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3158663.

Digital Object Identifier 10.1109/TII.2022.3158663

I. Introduction

SMART grid infrastructure (SGI) is on its way to taking over the traditional power systems due to its harmonious integration of information and communication technologies with the power generation and distribution systems. Through the usages of bidirectional cyber communication, the SGI manages the on-demand power flow from power generation sources to the domestic and industrial consumers. The SGI controls and optimizes the power supply according to real-time consumer demands through its power management capabilities. The SGI entities, including the smart meters (SMs) and neighbor-hood network area (NAN), are equipped with sensing devices along with transmitters and receivers for bidirectional exchange of power-related information [1].

The SGI is an advanced infrastructure and is more reliable than the conventional grid. SGI enhances efficiency through the use of artificial intelligence and automation features. Moreover, it facilitates the consumers with cost effectiveness. The SGI can also provide the flexibility to integrate the distributed power generation sources, which is challenging in conventional tasks. The SMs are typically installed at open spaces outside the apartments/industrial units, and such open installations can lead to physical attacks alongside the cyberattacks. The attacker can tap the public communication channel and expose consumption-related data for malicious usage. The exposed information can be harmful to user privacy, and it can disclose that when users are at home and when the home is vacant, the attacker can pose several threats to the affected building using this information. The attacker can also forge the consumption-related data by controlling the public channel, including the billing information. The attacker can also disrupt the power supply and fluctuate the electricity. In 2015, the attacker/s, by launching a cyberattack, successfully disconnected the power for the citizens of Ukraine for some hours. The main cause of the successful attack was exploiting the authentication mechanism by the attacker. Consequently, the attacker controlled the whole SGI [2]. This calls for a robust authentication scheme to support secure communication and information exchange among an SM and NAN gateway and protect user privacy.

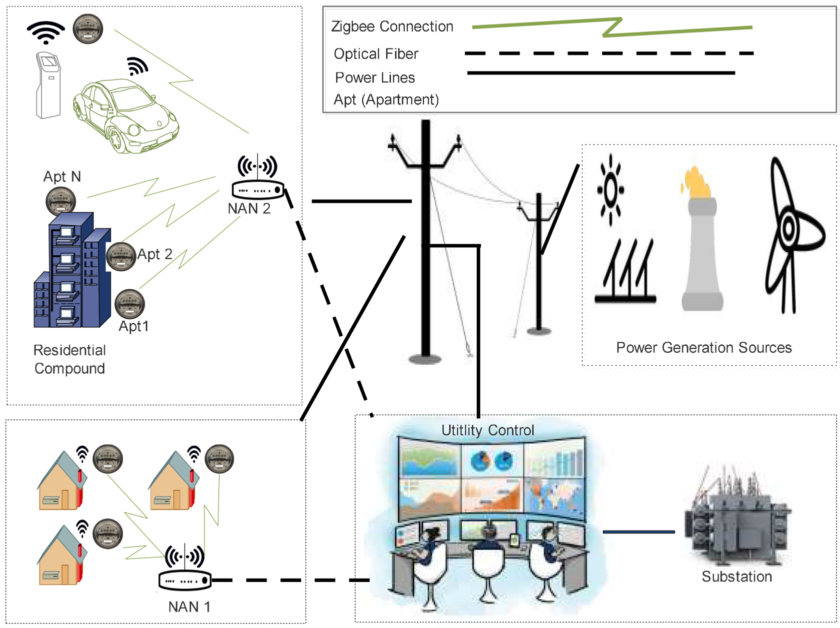

Fig. 1. Smart grid infrastructure.

A. Article Organization

The rest of this article is organized as follows. Section I-B explains the motivations and contributions of this study, followed by the system model in Section I-C, whereas the Section I-D briefs the adversary model. The existing and related works are summarized in Section II, and Section III explains the proposed lightweight authentication scheme for smart grid (LAS-SG) scheme. The formal security proof and description, along with the automated validation of the LAS-SG security, are given in Section IV. The comparisons related to computation, communication costs, and security features between proposed LAS-SG and related schemes are given in Section V. Finally Section VI concludes this article.

B. Motivation and Contributions

The communication structure underlying the SGI is the public internet, leading to several types of forgery attacks. Due to weaknesses of some existing security methods for SGI, the consumers and electricity providers can be exploited by malicious activities. Instead of advantages, the SGI could have become prey to incorrect demand response settings and forecasting. Even such attacks can lead to loss of electrical equipment and human loss. The insecurities of the existing schemes call for a secure and privacy-preserving authentication scheme for SGI. Following are the contributions of this study.

1) We design and present a lightweight authentication scheme for smart grid infrastructure (LAS-SG) using elliptic curve cryptography (ECC) and symmetric key encryption, and one-way message authentication operations. The *LAS-SG* avoids resource-extensive pairing and other operations. The *LAS-SG* accomplishes the authentication process by exchanging only two messages among a SM and NAN gateway.
2) We proved the attack resilience of the proposed *LAS-SG* against several malicious attacks using the formal random oracle model (ROM) as well as through an informal discussion.
3) The performance and security features of the *LAS-SG* are compared with some of the latest and related schemes.

C. System Model

The SGI system model, as portrayed in Fig. 1, includes NAN gateways, corresponding SMs, utility center, power connections, and power generation sources in typical hierarchical settings. The NANs and SMs are connected through ZigBee channels, whereas NANs and utility centers connect through optical fiber for fast communication. The SMs gather the real-time consumption demands and communicate with NAN gateways to adjust the electricity usage. Both the SMs and NAN gateways accommodate the two-way communication for sending and receiving the consumption demand and response messages. Before initiating the authentication, each SM must register with the corresponding NAN gateway.

D. Adversary Model

This article considers the standard eCK [11] attack model and in eCK model, the attacker has more powers as compared with DY [12] and CK models [13]. In eCK model, the adversary, in addition to having full authority, such as sending a forged message, receiving/listening to the communicated messages, blocking the messages over the insecure communication channel, can also execute a key compromise impersonation attack. The attacker can extract data stored in the memory of an SM. Only NAN is trusted, whereas any SM can try to deceive a NAN and cannot be trusted. The attacker has access to all public system parameters.

II. Related Work

Public key-based infrastructure (PKI) is a very popular approach, which is being used for SGI security. Initially, in this context some one-way authentication schemes were proposed [14]–[17]. In one-sided authentication schemes, the authenticity of the initiator (SM) is always verified before establishing a secure channel and exchanging a session key. However, this sort of one-sided authentication is not feasible and can pose various security weaknesses due to the nonverification of the responder (NAN gateway). The weaknesses of the one-way authentication schemes paved the way for the design of a two-way authentication scheme, and in this context, some PKI-based authentication schemes were proposed [3]–[7], [9], [18]–[21]. Mahmood et al. [4] presented a pairing and ECC-based two-way authentication scheme, but due to pairing, the scheme cannot cope with the lightweightness requirements of the SGI. Moreover, Liang et al. [22] in their study also proved that the scheme presented in [4] is weak against impersonation and ephemeral secret leakage attacks. Tasi and Lu [3] also used ECC and pairing operations to propose a new authentication scheme for SGI. In their scheme, Tasi and Lu [3] avoided costly pairing operations to extend computational efficiency for the SM. However, the scheme [3] uses pairing operations along with ECC on NAN gateways. Although Tasi and Lu [3] tried to provide computational efficiency on the SM due to usage of pairings on the NAN gateway, the computational cost of the scheme of Tsai and Lu [3] was still high. Moreover, Odelu et al. [5] also proved the weaknesses of the scheme of Tsai and Lu [3] against ephemeral secret leakage attack (ESLA). The schemes of Tsai and Lu[3] and Odelu et al. have weaknesses against impersonation, a man in the middle, and DoS attacks. Another scheme in a three-party setting was also proposed by Challa et al. [18]. Kumar et al. [7] also proposed an ECC-based authentication scheme for SGI. However, Chaudhry et al. [19] argued that the scheme presented in [18] has a faulty design, and due to the incorrectness, their scheme cannot complete even a round of authentication. Likewise, Chaudhry et al. [23] also proved that the scheme presented in [7] is built on faulty design and cannot facilitate SM and NAN gateways to share a session key. Chaudhry et al. [9] also proposed an ECC- and certificate-based authentication scheme for managing demand-response in SGI. However, if an attacker or a deceitful SM owner ($\mathcal{A}$) physically extracts the parameters $\{\mathrm{ID}_i, \mathrm{RID}_i, C_i, Q, P_{uj}\}$, where $C_i = x + H(\mathrm{ID}_i||Q)x$ stored in an SM. It can easily extract the private key of the utility control center (UC). For computing private key of UC, $\mathcal{A}$ using extracted ID_i, Q, and C_i computes $\Omega = (1 + H(\mathrm{ID}_i||Q))^{-1}$. As we know $C_i = x + H(\mathrm{ID}_i||Q)x$, and it can be represented as $C_i = x(1 + H(\mathrm{ID}_i||Q)$. Now, $\mathcal{A}$ can compute the private key of the UC by multiplying Ω with C_i, i.e., $x = \Omega.C_i = (1 + H(\mathrm{ID}_i||Q))^{-1}.(1 + H(\mathrm{ID}_i||Q))$, where x is the private key of the UC. In 2020, Khan et al. [10] also proposed another protocol using ECC. However, as per the analysis performed in [24], the scheme of Khan et al. [10] cannot complete a cycle of authentication procedure due to a superficial point multiplication operation over an elliptic curve. Moreover, Chaudhry et al. [25] proved that Garg et al. [8] cannot resist key compromise impersonation attack, and it lacks forward secrecy and anonymity. Yahya et al. [26] evaluated the scheme lightweight authentication and key agreement (LAKA) using ECC by Kumar et al. [6]. They proved that the LAKA scheme of Kumar et al. has insecurities against ESLA, stolen verifier, and traceability attacks. As per the analysis conducted in several studies, most of the existing schemes for SGI security are either insecure against one or more security weaknesses or cannot cope with the resource-constrained nature of SGI. The integrity of the messages transmitted over insecure public channels and performance efficiency are two fundamental requirements for realizing the advantages of the SGI. In these absences, irregular, delayed, or incorrect decisions can be substantiated for SGI. Table I summarizes the limitations of the existing related schemes.

III. Proposed Scheme: LAS-SG

The description of the proposed LAS-SG is briefed in the following sections.

A. Setup Phase

The NAN-gateway is considered trusted, and NAN is anticipated to furnish offline tasks, which encompasses the assignment of 1) identity to each SM, 2) security parameters, and 3) tracking the log-records. The following are the security parameters of the NAN for setting up the system. To initiate the setup process, the NAN opts for an E, which is an elliptic curve along over the finite field F_p and a point P on E with an order n. In addition, NAN opts for a master secret key and public key pair M_k and $P_s = M_k.P$ along with a hash function $H()$. The NAN publishes $\{E, P, F_p, n, H(), P_s\}$ and keeps M_k confidential.

B. Registration Phase

Before inclusion into a clientage of a NAN gateway, the SM has to register with the NAN. The process accomplishes by the NAN, and for this, the NAN generates unique identities $\{\mathrm{SM}_{\mathrm{ID}_j} : j = 1, 2...x\}$ for each of the SM (j). The NAN then using $\mathrm{SM}_{\mathrm{ID}_j}$ computes $\sigma_j = H(\mathrm{SM}_{\mathrm{ID}_j})$ along with a public key ($\mathrm{SMpub}_j = (\sigma_j + M_k).P = \sigma_j P + P_s$) for the jth SM. The NAN then computes a token $\mathrm{ST}_j = h(\mathrm{SM}_{ID_j}||M_k||\mathrm{SM}_{\mathrm{Pr}_j})$ secret/private for $\mathrm{SM}_{\mathrm{ID}_j}$ and a unique identifier $\mathrm{id}_{\mathrm{ST}_j}$. The NAN subsequently uses M_k and computes $\mathrm{SMpr}_j = \frac{1}{M_k+\sigma_j}.P \in G$ is the private key corresponding to the SM's public key SMpub_j. For each $\{\mathrm{SM}_j : j = 1, 2...n\}$, where n is the total number of registered SMs. The NAN also computes $Pid_{\mathrm{st}_j} = E_{Mk}(\mathrm{id}_{\mathrm{st}_j}, r_n)$ and stores $\{E, P, F_p, n, \mathrm{SMpr}_j, \sigma_j, \mathrm{id}_{\mathrm{ST}_j}, \mathrm{ST}_j, H(..)\}$ in the memory of temper proof SM. The NAN also stores $\mathrm{SM}_{\mathrm{ID}_j}$ and $Pid_{\mathrm{st}j}$ in the SM's memory. Finally, all the registered SMs are deployed at desired locations.

C. Authentication Phase

To provide a lightweight authentication mechanism, the following procedure, as illustrated in Fig. 2, is explained as follows.

PAK 1: The $\mathrm{SM}_{\mathrm{ID}_j}$ initiates the authentication process by computing $A_{\mathrm{SM}_j} = u_{\mathrm{SM}_j}.P$, $B_{\mathrm{SM}j} = u_{\mathrm{SM}j}.\mathrm{SM}_{\mathrm{pr}j}$, $L1 = H(\mathrm{SM}_{\mathrm{ID}j}||A_{\mathrm{SM}j}||B_{\mathrm{SM}j}||T1)$, $Q1 = E_{\mathrm{ST}j}[\mathrm{SM}_{\mathrm{ID}j}, T1]$, and $Y1 = \mathrm{MAC}_{L1}[\mathrm{SM}_{\mathrm{ID}j}, T1, A_{\mathrm{SM}j}, \mathrm{ST}_j]$. The $\mathrm{SM}_{\mathrm{ID}_j}$ then

TABLE I
SUMMARY OF RELATED WORKS

Scheme	Year	CTU	Weaknesses
Tsai and Lu [3]	2016	ECC& EXP	Heavy Computation cost and weak against ESLA, MIM, IMP and DoS attacks.
Mahmood et al. [4]	2018	EBP	Weak against IMP and ESLA attacks.
Odelu et al. [5]	2018	ECC& EXP	Heavy Computation cost and weak against ESLA, MIM, IMP and DoS attacks.
P. Kumar et al. [6]	2018	ECC	Weak against ESLA, stolen verifier, and traceability attacks.
N. Kumar et al. [7]	2019	ECC	The scheme has incorrect login and authentication phase.
Garg et al. [8]	2019	ECC	Weak against KCI and does not provide PFS, user anonymity.
Chaudhry et al. [9]	2020	ECC	Weak against physical capturing attack.
Khan et al. [10]	2020	ECC	The scheme has incorrect login and authentication phase.

CTU: cryptographic technique used; ECC: elliptic curve cryptography, EBP: ECC-based bilinear pairing; EXP: exponentiation; ESLA: ephemeral secret leakage attack; MIM: man in middle; IMP: impersonation; KCI: key compromise impersonation; PFS: perfect forward secrecy.

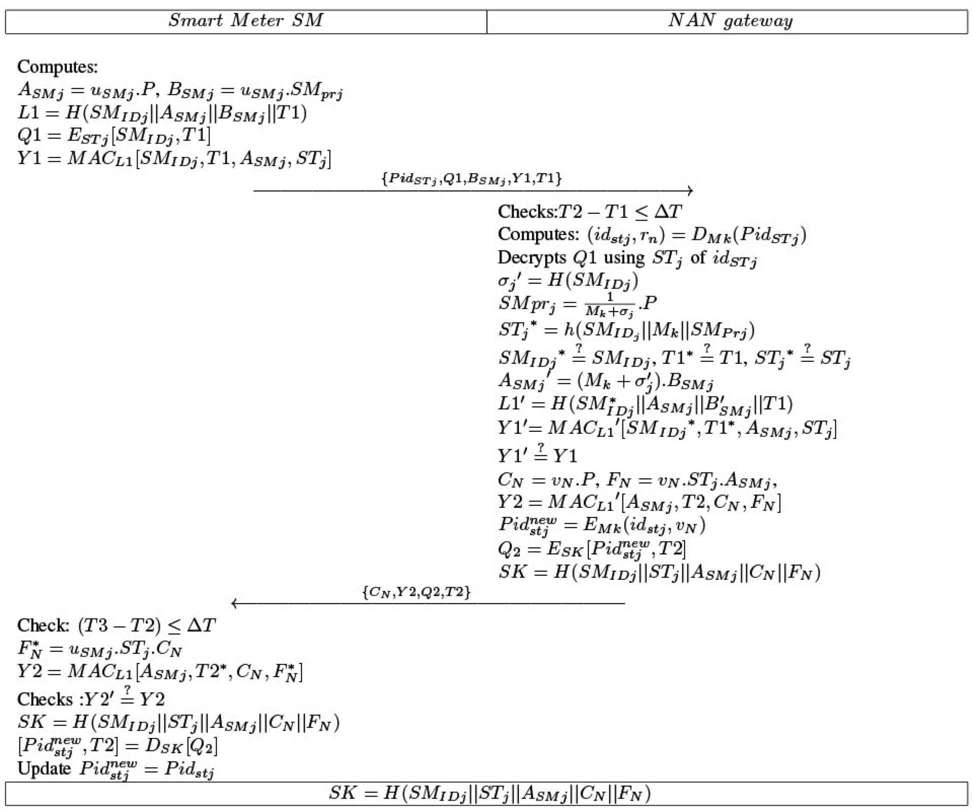

Fig. 2. Flow of proposed LAS-SG.

sends $\{Pid_{STj}, Q1, B_{SMj}, Y1, T1\}$, where $T1$ is the current timestamp extracted at SM.

PAK 2: The NAN checks the validity of $T1$ by comparing it with current timestamp extracted at NAN. If $T2 - T1 \leq \Delta T$, the NAN computes $(\mathrm{id}_{stj}, r_n) = D_{Mk}(Pid_{STj})$, where ΔT is the tolerable delay and Mk is the master secret key of the NAN gateway. The NAN then decrypts $Q1$ using ST_j of id_{STj} and gets SM_{IDj} and $T1$. The NAN then computes $\sigma_j{}' = H(\mathrm{SM}_{IDj})$, $\mathrm{SMpr}_j = \frac{1}{M_k+\sigma_j}.P$, and $\mathrm{ST}_j{}^* = h(\mathrm{SM}_{ID_j}||M_k||SM_{Prj})$. The NAN then checks $\mathrm{SM}_{IDj}{}^* \stackrel{?}{=} \mathrm{SM}_{IDj}$, $T1^* \stackrel{?}{=} T1$, and $\mathrm{ST}_j{}^* \stackrel{?}{=} \mathrm{ST}_j$, and on successful validation, the NAN computes $A_{SMj}{}' = (M_k + \sigma'_j).B_{SMj}$, $L1' = H(\mathrm{SM}^*_{IDj}||A_{SMj}||B'_{SMj}||T1)$, $Y1' = \mathrm{MAC}_{L1}{}'[\mathrm{SM}_{IDj}{}^*, T1^*, A_{SMj}, \mathrm{ST}_j]$. Now, NAN checks the validity of $Y1' \stackrel{?}{=} Y1$, and on successful validation, the NAN computes $C_N = v_N.P$, $F_N = v_N.\mathrm{ST}_j.A_{SMj}$, $Y2 = \mathrm{MAC}_{L1}{}'[A_{SMj}, T2, C_N, F_N]$, $Pid^{new}_{stj} = E_{Mk}(\mathrm{id}_{stj}, v_N)$, $Q_2 = E_{SK}[Pid^{new}_{stj}, T2]$, and the session key $\mathrm{SK} = H(\mathrm{SM}_{IDj}||\mathrm{ST}_j||A_{SMj}||C_N||F_N)$. The NAN finally sends $\{C_N, Y2, Q2, T2\}$ to SM_{ID_j}.

PAK 3: The SM_{ID_j} on receiving the message checks the validity of $T2$ by comparing it with current timestamp extracted at SM_{ID_j}. If $(T3 - T2) \leq \Delta T$, the SM_{ID_j} computes $F^*_N = u_{SMj}.\mathrm{ST}_j.C_N$ and $Y2 = \mathrm{MAC}_{L1}[A_{SMj}, T2^*, C_N, F^*_N]$, where ΔT is the tolerable delay. The SM_{ID_j} now checks the validity of $Y2' \stackrel{?}{=} Y2$ and

TABLE II
QUERIES AND THEIR ANSWERS

$\boldsymbol{Set-up}$: $\mathcal{R}$ sends system parameters to $\mathcal{A}$ as an answer to this query.
$\boldsymbol{h(x_i)}$: $\mathcal{R}$ chooses r_i randomly, add $\{x_i, r_i\}$ in the list H_l and sends r_i to $\mathcal{A}$ as answer to this query.
$\boldsymbol{Send(SG^a, M_a)}$ **:** $\mathcal{R}$ answers as per the protocol specification of the proposed *LAS-GS*, on reception M_a, which is sent by $\mathcal{A}$.
$\boldsymbol{CorruptSM}$: When this query is executed using the identity (SM_{IDj}) of a SM, the $\mathcal{R}$ answers with the private key SM_{prj} of SM to $\mathcal{A}$.
$\boldsymbol{Reveal(P^x)}$: Using this query, $\mathcal{A}$ can get the session key computed among an instance SG^a of a SM and another instance SG^b of NAN gateway during x^{th} execution of protocol P.
$\boldsymbol{Test(SG^a)}$: $\mathcal{R}$ answers with the outcome of a coin flip c experiment on asking of the session key by $\mathcal{A}$ thorough execution of this query.

on successful validation, the SM_{ID_j} computes the session key $\text{SK} = H(\text{SM}_{\text{ID}j}||\text{ST}_j||A_{\text{SM}j}||C_N||F_N)$ and $[Pid^{\text{new}}_{\text{st}j}, T2] = D_{\text{SK}}[Q_2]$ and updates $Pid^{\text{new}}_{\text{st}j} = Pid_{\text{st}j}$.

IV. Security Analysis

The provable formal security under ROM [27] is adopted in this article to prove the robustness of the proposed LAS-SG. The evidence that *LAS-SG* resists many attacks and provides adequate security is given in the following sections.

A. Security Model

We adopted the security model as utilized in [28]–[30]. Under the adopted security model, the attacker $\mathcal{A}$ communicates with SG^a, the ath instance of the SG entity (SM or NAN gateway). Under the adopted security model, $\mathcal{A}$ sends several queries to the responder $\mathcal{R}$ and $\mathcal{R}$ correspondingly sends the answers to $\mathcal{A}$. The queries and their answers are given in Table II.

To break the security of *LAS-SG*, $\mathcal{A}$ tries to guess the value of coin flipping c' and $\mathcal{A}$ succeeds in breaking security of *LAS-SG* if the guessed $c' = c$. We consider E_{GC} as the event where $\mathcal{A}$ has guessed c correctly. The advantage undertaken by $\mathcal{A}$ can be represented as $Adv^{\text{AKA}}_{\text{LAS-SG}}(\mathcal{A}) = |2\text{Pr}[E_{\text{GC}}] - 1|$. Some of the definitions are as follows.

Definition 1 ($AKA^{SMj}_{NAN} - Secure$): The LAS-SG protocol P is $\text{AKA}^{\text{SM}j}_{\text{NAN}} - \text{Secure}$ if $Adt^{\text{AKA}}_{\text{LAS-SG}}(\mathcal{A})$ is negligible.

The protocol (*LAS-SG*) is MA-secure among an SM and NAN if and only if $\mathcal{A}$ being an attacker cannot produce any one of the ① initial message $M_1\{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$ legitimately generated by SM and ② reply message $\{C_N, Y2, Q2, T2\}$ legitimately generated by NAN gateway. We denote E_{SN} and E_{NS} as the events, where $\mathcal{A}$ can produce $M_2 = \{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$ and $\{C_N, Y2, Q2, T2\}$, respectively. The advantage that $\mathcal{A}$ have to break LAS-SG's MA security is solicited as follows: $Adt^{\text{MA}}_{\text{LAS-SG}}(\mathcal{A}) = \text{Pr}[E_{\text{SN}}] + \text{Pr}[E_{\text{NS}}]$.

Definition 2 ($MA^{SM}_{NAN} - Secure$): The LAS-SG protocol $\mathcal{P}$ is $\text{MA}^{\text{SM}}_{\text{NAN}} - \text{Secure}$ if the $Adt^{\text{MA}}_{\text{LAS-SG}}(\mathcal{A})$ is negligible.

B. Provable Security

The security of the *LAS-SG* is proved in this section by taking into consideration the security model explained in the abovementioned section.

Theorem 1: The *LAS-SG*-proposed scheme achieves mutual authentication.

Proof: At first glance, $\mathcal{A}$ can execute $\text{Send}(\text{SM}, M_1)$ and in case the responder $\mathcal{R}$ is able to get verify $\text{ST}_j{}^* \stackrel{?}{=} h(\text{SM}_{\text{ID}_j}||M_k||\text{SM}_{\text{Pr}j})$, and $Y1' \stackrel{?}{=} \text{MAC}_{L1}{}'[\text{SM}_{\text{ID}j}{}^*, T1^*, A_{\text{SM}j}, \text{ST}_j]$, then M_1 is legitimate, where $M_1 = \{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$. The freshness and validity of M_1 can be checked by $\mathcal{R}$ by using M_k and $\text{SMpr}_j = \frac{1}{M_k+\sigma_j}.P$, which are private keys of NAN and SM, respectively. $\mathcal{R}$ explores the list H_l and gets a record with probability $1/q_h$ and another record for M_l with probability $1/q_m$. Therefore, $\mathcal{A}$ can produce forged message M_1. The probability of the event E_{SN} for $\mathcal{A}$ to forge M_1 is $\text{Pr}[E_{\text{SN}}] = 1/(q_h.q_m)$. In a similar manner, $\mathcal{A}$ can attempt to forge M_2 by executing $\text{Send}(\text{NAN}, M_2)$. In this case, if $\mathcal{R}$ could successfully be able to verify $Y2 = \text{MAC}_{L1}[A_{\text{SMj}}, T2^*, C_N, F^*_N]$, then M_2 is legitimate, where $M_2 = \{C_N, Y2, Q2, T2\}$. The $\mathcal{R}$ gets a record from the list M_l and its' probability is $1/q_m$. In case, two legitimate messages $\{C_N, Y2, Q2, T2\}$ and $\{\overline{C}_N, \overline{Y2}, \overline{Q2}, T2\}$ are produced, the $\mathcal{R}$ can then compute $(u_{\text{SM}j} - \overline{u}_{\text{SM}j}).P$ and event-probability of $\text{Pr}[E_{\text{NA}}] = 1/(p.q_h.q^2_m)$. Hence, it be inferred that $Adt^{\text{MA}}_{\text{LAS-SG}}(\mathcal{A})$ is negligible.

Theorem 2: The *LAS-SG* is secure semantically if the discrete logarithm problem of the ECC is hard.

Proof: The $\mathcal{R}$ can have nonnegligible advantage ϵ on execution of Test query for computing correct session key $\text{SK} = H(\text{SM}_{\text{ID}j}||\text{ST}_j||A_{\text{SM}j}||C_N||F_N)$, and event E_{SK} is the representation of correctly computing the SK. During execution of test query, the $\mathcal{A}$ guesses the outcome of c with probability $\geq 1/2$. Therefore, $\text{Pr}[E_{\text{sk}} \geq \epsilon/2$. Now, consider $E^{\text{SM}}_{\text{Test}}$ and $E^{\text{NAN}}_{\text{Test}}$ are the representation of the events that SM and NAN both are queried tby Test. Therefore, we get the following:

$$\epsilon/2 \leq \text{Pr}[E_{\text{sk}}] \tag{1}$$

$$= \text{Pr}[E_{\text{sk}} \wedge E^{\text{SM}}_{\text{Test}}] + \text{Pr}[E_{\text{sk}} \wedge \quad E^{\text{NAN}}_{\text{Test}} \wedge E_{\text{SN}}]$$

$$+ \text{Pr}[E_{\text{sk}} \wedge E^{\text{NAN}}_{\text{Test}} \wedge \neg E_{\text{NS}}]$$

$$\text{Pr}[E_{\text{sk}} \wedge E^{\text{SM}}_{\text{Test}}] + \text{Pr}[E_{\text{sk}} \wedge \quad E^{\text{NAN}}_{\text{Test}} \wedge \neg E_{\text{SN}}]$$

$$\leq \epsilon/2 - \text{Pr}[E_{\text{SN}}] \tag{2}$$

Since $\text{Pr}[E^{\text{NAN}}_{\text{Test}} \wedge \neg E_{\text{SN}} = E^{\text{SM}}_{\text{Test}}$, therefore,

$$\text{Pr}[\text{SK} = H(\text{SM}_{\text{ID}j}||\text{ST}_j||A_{\text{SM}j}||C_N||F_N)] \geq \epsilon/4 - \text{Pr}[E_{\text{SN}}]/2. \tag{3}$$

1) SM Impersonation Attack: $\mathcal{A}$ may try to forge initial request message M_1 to impersonate itself as a legitimate SM. For impersonation, $\mathcal{A}$ tries to produce the forged but valid message $M_1 = \{Pid^{\mathcal{A}}_{\text{ST}j}, Q1^{\mathcal{A}}, B^{\mathcal{A}}_{\text{SM}j}, Y1^{\mathcal{A}}, T1^{\mathcal{A}}\}$ on behalf of SM. For this $\mathcal{A}$ can select a random number $u^{\mathcal{A}}_{\text{SM}j}$ and can compute $A^{\mathcal{A}}_{\text{SM}j} = u^{\mathcal{A}}_{\text{SM}j}.P$ but for computing $B^{\mathcal{A}}_{\text{SM}j} = u^{\mathcal{A}}_{\text{SM}j}.\text{SM}_{\text{pr}j}$, the attacker needs private key of the SM. Moreover, referring to Theorem 1, $\mathcal{A}$ cannot construct a valid M_1, which can satisfy both ① $\text{ST}_j{}^* \stackrel{?}{=} h(\text{SM}_{\text{ID}_j}||M_k||\text{SM}_{\text{Pr}j})$ and ②

$Y1' \stackrel{?}{=} \text{MAC}_{L1}'[\text{SM}_{\text{ID}j}{}^*, T1^*, A_{SMj}, ST_j]$, without having private key $\text{SM}_{\text{pr}j}$ and secret token ST_j of the SM with non-negligible advantage. Therefore, proposed LAS-SG resists SM impersonation attack.

2) NAN Impersonation Attack: $\mathcal{A}$ can also try to impersonate on behalf of NAN gateway and for this, $\mathcal{A}$ may construct reply message $M_2^{\mathcal{A}} = \{C_N^{\mathcal{A}}, Y2^{\mathcal{A}}, Q2^{\mathcal{A}}, T2^{\mathcal{A}}\}$ by generating fresh time-stamp $T2^{\mathcal{A}}$ and sending the forged but valid message $M_2^{\mathcal{A}}$ to SM. However, the message $M_2^{\mathcal{A}}$ constructed by $\mathcal{A}$ must pass $Y2 \stackrel{?}{=} \text{MAC}_{L1}[A_{\text{SM}j}, T2^*, C_N, F_N^*]$, and as per Theorem 2, $\mathcal{A}$ cannot construct valid M_2 without having access to private key M_k, $\mathcal{A}$ has negligible advantage for completion of this task. Therefore, $\mathcal{A}$ cannot impersonate on behalf of a NAN gateway.

3) Anonymity and Untraceability: In *LAS-SG*, $\mathcal{A}$ cannot expose user identity during message exchanges. Moreover, $\mathcal{A}$ is not able to trace the requesting user. In each request message, the encrypted $\text{id}_{\text{st}j}$ and in each round of authentication $\text{id}_{\text{st}j}$ is encrypted along with a session-specific random number using the master secret key M_k of the NAN gateway. The statistically independent $Pid_{\text{ST}j}$ is computed in each session. Therefore, *LAS-SG* is not only anonymous but also provides untraceability for the SM.

4) Key Compromise Impersonation Attack: In *LAS-SG*, the $\mathcal{A}$ can get private key of SM and can impersonate itself on behalf of the noncompromised NAN. Let $\mathcal{A}$ has the private key and related parameters $\{\text{ST}_j, \text{id}_{\text{ST}_j}, \sigma_j, \text{SMpr}_j, \text{SM}_{\text{ID}_j}, Pid_{\text{st}j}\}$ of SM. The $\mathcal{A}$ waits for the SM_{ID_j} to initiate the login requests and it blocks the request, once initiated. The $\mathcal{A}$ reads the login parameters $\{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$. The $\mathcal{A}$ may construct reply message $M_2^{\mathcal{A}} = \{C_N^{\mathcal{A}}, Y2^{\mathcal{A}}, Q2^{\mathcal{A}}, T2^{\mathcal{A}}\}$ by generating fresh time-stamp $T2^{\mathcal{A}}$ and sending the forged but valid message $M_2^{\mathcal{A}}$ to SM_{ID_j}. For this, $\mathcal{A}$ has to construct $M_2^{\mathcal{A}}$ which must pass $Y2 \stackrel{?}{=} \text{MAC}_{L1}[A_{\text{SM}j}, T2^*, C_N, F_N^*]$. Moreover, for decryption of $Pid_{\text{ST}j}$ and formation of $A_{\text{SM}j} = (M_k + \sigma_j).B_{\text{SM}j}$, the attacker $\mathcal{A}$ also needs M_k. As per Theorem 2, $\mathcal{A}$ cannot construct valid M_2 without having access to private key M_k. Similarly, the possession of private key and related parameters $\{\text{ST}_j, \text{id}_{\text{ST}_j}, H(), \sigma_j, \text{SMpr}_j, \text{SM}_{\text{ID}_j}, Pid_{\text{st}j}\}$ of SM_{ID_j} extends no advantage to compute $\{Y2, C_N\}$ pair. Therefore, for construction of verifiable M_2 without having access to private key M_k of the NAN, the $\mathcal{A}$ has negligible advantage. Hence, it can be concluded that the proposed resists key compromise impersonation attack.

5) Man in Middle Attack: In *LAS-SG*, the $\mathcal{A}$ can try to launch the man in middle attack (MIMA), and for this $\mathcal{A}$ can wait for SM to initiate login. The $\mathcal{A}$ captures from the public channel $\{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$, and try to send forged message $\{Pid_{\text{ST}j}^{\mathcal{A}}, Q1^{\mathcal{A}}, B_{\text{SM}j^{\mathcal{A}}}, Y1^{\mathcal{A}}, T1^{\mathcal{A}}\}$ to NAN gateway. Similarly, $\mathcal{A}$ can capture reply message $\{C_N, Y2, Q2, T2\}$ and try to send the forged message $\{C_N^{\mathcal{A}}, Y2^{\mathcal{A}}, Q2^{\mathcal{A}}, T2^{\mathcal{A}}\}$. However, as per Theorem 1, $\mathcal{A}$ cannot construct both ① the forged request and ② the forged reply message. Therefore, *LAS-SG* resists MIMA attack.

6) SM Physical Capture Attack: The SM can be captured physically and the $\mathcal{A}$ can extract the parameters $\{\text{ST}_j, \text{id}_{\text{ST}_j}, H(), \sigma_j, \text{SMpr}_j\}$ stored in SM, these parameters cannot be used to impersonate any of the noncompromised SM or NAN. Therefore, physical capturing of an SM does not affect the security of the *LAS-SG* scheme, and our scheme resists physical capturing of SMs.

7) Replay Attack: In *LAS-SG*, the request message $\{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$ contains current timestamp $T1$ in plaintext as well as it is embedded in encrypted $Q1 = E_{\text{ST}j}[\text{SM}_{\text{ID}j}, T1]$. If an attacker replays an old message or send the modified message by replacing $T1$, it will be caught immediately. Therefore, *LAS-SG* resists replay attack.

8) Perfect Forward Secrecy: In *LAS-SG*, the session key $\text{SK} = H(\text{SM}_{\text{ID}j}||\text{ST}_j||A_{\text{SMj}}||C_N||F_N)$ is constructed using both secret session parameters $A_{\text{SM}j}$ and F_N and long-term secret ST_j. If any of the long-term and session parameters are exposed to adversary, the computation of session key is not feasible and *LAS-SG* provides perfect forward secrecy.

9) Known Session Key: In *LAS-SG*, the session keys are independent to each other and due to the usage of session-specific random parameters and one-way hash function, even if one session key $\text{SK}^1 = H(\text{SM}_{\text{ID}j}^1||\text{ST}_j^1||A_{\text{SM}j}^1||C_N^1||F_N^1)$ is exposed to SM, it has no affect on any other session key $\text{SK}^2 = H(\text{SM}_{\text{ID}j}^2||\text{ST}_j^2||A_{\text{SM}j}^2||C_N^2||F_N^2)$.

TABLE III
EXPERIMENTAL RUNNING TIMES

↓Device/RT→	T_{pb}	T_{em}	T_{ex}	T_{ea}	T_{ow}	T_{sc}
SM	12.52	4.107	6.143	0.018	0.006	2.011
NAN	4.038	0.926	1.40	0.006	0.004	0.118

RT: Running time in milliseconds.

C. Automated Analysis Through ProVerif

In this section, we briefly describe the evaluation results of the ProVerif analysis applied on the proposed *LAS-SG*. The ProVerif is a widely used formal and automated verification tool, and its security validation analysis is built on applied π-calculus. The application of ProVerif is categorized into following three parts.

① The declaration part includes the presentation of constants, variables, channels (public and private), equations, and constructors.

② The processes simulate the distributed procedures of each of the entities.

③ The main part includes the queries and initiation and termination of the parallel process.

We simulated the two processes and queries as per the specifications of the original *LAS-SG* protocol. The simulation results are as follows.

1) RESULT inj − event(end_SM(IDSM[]) ==> inj − event(start_ SM(IDSM[]) is true.
2) RESULT inj − event(end_NAN(IDNAN[])) ==> inj − event(start_ NAN(IDNAN[])) is true.
3) RESULT not attacker(SK[]) is true.

The verification outputs ① and ② depict that SM and NAN processes initiated and finished normally, and output ③ indicates that session key (SK) is not revealed to the attacker.

TABLE IV
PERFORMANCE COMPARISONS

Scheme	SM	NAN	RT	ME	BE
Mahmood et al. [4]	$T_{pb} + 2T_{pm} + T_{ex} + 3T_{ow}$	$2T_{pb} + 2T_{pm} + T_{ex} + 4T_{ow}$	≈ 39.165	3	180
Odelu et al. [5]	$3T_{pm} + T_{ex} + 6T_{ow}$	$2T_{pb} + 2T_{pm} + T_{ex} + 6T_{ow}$	≈ 29.852	3	160
Tsai and Lu [3]	$4T_{pm} + T_{ex} + 5T_{ow}$	$2T_{pb} + 3T_{pm} + T_{ex} + 5T_{ow}$	≈ 34.875	3	180
N. Kumar et al. [7]	$2T_{pm} + 6T_{ow}$	$2T_{pm} + 6T_{ow}$	≈ 10.126	3	148
Chaudhry et al. [9]	$3T_{pm} + 3T_{ow}$	$5T_{pm} + 2T_{ea} + 4T_{ow}$	≈ 16.993	2	156
P. Kumar et al. [6]	$3T_{pm} + 4T_{sc} + 6T_{ow}$	$3T_{pm} + 4T_{sc} + 7T_{ow}$	≈ 23.679	2	272
Khan et al. [10]	$4T_{pm} + 11T_{sc} + 10T_{ow}$	$4T_{pm} + 11T_{sc} + 9T_{ow}$	≈ 43.647	2	392
Garg et al. [8]	$3T_{pm} + T_{ea} + 5T_{ow}$	$3T_{pm} + T_{ea} + 5T_{ow}$	≈ 15.172	2	156
LAS-SG	$3T_{pm} + 2T_{sc} + 4T_{ow}$	$4T_{pm} + 2T_{sc} + 6T_{ow}$	≈ 20.331	2	192

RT: running time in milliseconds, ME: number of message exchanges, BE: bytes exchanges.

TABLE V
SECURITY FEATURES

	[4]	[5]	[3]	[7]	[9]	[6]	[10]	[8]	Our
$\mathcal{X}_1$	√	√	√	•	√	√	•	√	√
$\mathcal{X}_2$	√	√	√	√	√	•	√	•	√
$\mathcal{X}_3$	•	•	•	√	√	√	√	√	√
$\mathcal{X}_4$	√	•	•	√	√	√	√	√	√
$\mathcal{X}_5$	•	√	•	√	√	•	√	√	√
$\mathcal{X}_6$	√	•	•	√	√	√	√	√	√
$\mathcal{X}_7$	√	√	√	√	√	•	√	√	√
$\mathcal{X}_8$	√	√	√	√	√	√	√	•	√
$\mathcal{X}_9$	√	√	√	√	√	√	√	√	√
$\mathcal{X}_{10}$	√	√	√	√	√	√	√	•	√
$\mathcal{X}_{11}$	√	√	√	√	√	√	√	√	√
$\mathcal{X}_{12}$	√	√	√	√	√	√	√	√	√
$\mathcal{X}_{13}$	√	√	√	√	•	√	√	√	√

Note: $\mathcal{X}_1$: correctness; $\mathcal{X}_2$: anonymity and untraceability; $\mathcal{X}_3$: resist impersonation; $\mathcal{X}_4$:resist man-in-middle; $\mathcal{X}_5$: ephemeral secret leakage; $\mathcal{X}_6$: denial of services; $\mathcal{X}_7$: stolen verifier; $\mathcal{X}_8$: resist key compromise impersonation; $\mathcal{X}_9$: resists replay; $\mathcal{X}_{10}$: perfect forward secrecy; $\mathcal{X}_{11}$: resist privileged insider; $\mathcal{X}_{12}$: session key security; $\mathcal{X}_{13}$: resist physical capture. √: secure or extends; •: insecure against or not provides.

V. COMPARISONS

The performance and security comparisons of the *LAS-SG* with some of the latest and related schemes [3]–[10] are solicited in the preceding sections.

A. Computation Cost

In this section, we compare the computation cost of our *LAS-SG* with related schemes [3]–[10], and for this purpose, we first introduce the following notations: T_{pb}, T_{em}, T_{ex} T_{ea}, T_{ow}, and T_{sc} represent bilinear pairing, ECC multiplication, exponentiation, ECC addition, one-way hash/MAC function, and symmetric key operation, respectively. To accumulate the computation cost, a real-time setup is organized. In our MIRACL library-based organized experiment, we used two devices: a Pi-3-B+ with Cortex A-53(ARMv.8) 64bits: SoC@1.4GHz-processor, with RAM specification of 1GB-LPDDR-2 SDRAM-RAM to replicate an SM. Similarly, the NAN was replicated using an HP Elite-Book 8460.P with Intel(R) Core-TM, 2.7-GHz (i7 2620-M), with 4GB RAM on Ubuntu: 16.0LTS OS. The running times on each of the devices are given in Table III. In proposed *LAS-SG* to furnish a round of authentication, the SM has to execute $3T_{\text{pm}} + 2T_{\text{sc}} + 4T_{\text{ow}}$ operations, in addition to the execution of $4T_{\text{pm}} + 2T_{\text{sc}} + 6T_{\text{ow}}$ operations by the NAN. Total execution time for a single round of authentication in the proposed *LAS-SG* is 20.331 ms. The schemes of Kumar et al. [6], Chaudhry et al. [9], Kumar et al. [7], Odelu et al. [3], Tsai and Lu [5], Mahmood et al. [4], Garg et al. [8], and Khan et al. [10] completed a single round of authentication in 23.679, 16.993, 10.126, 29.852, 34.875, 39.165, 15.172, and 43.647 ms, respectively. The proposed scheme has low computation cost as compared with other schemes [3]–[6], [10] and has extra computation cost/running time when compared with the existing schemes presented in [7]–[9].

B. Communication Cost

We have considered the following assumptions for communication cost comparisons: the identity and random token sizes are taken as 64 bits long, and timestamps are considered 32 bits of length. We have considered SHA-1 as the standard one-way function with size 160 bits. The ECC point with two coordinates is considered as 320 bits long, where each coordinate is 160 bits of length. The size of RSA is 1024 bits. We have selected advanced encryption standard (AES) symmetric encryption algorithm with a block size of 128 bits. The proposed *LAS-SG* completes a round of authentication procedures by exchanging two messages: $m_1\{Pid_{\text{ST}j}, Q1, B_{\text{SM}j}, Y1, T1\}$ and the reply message $m_2 = \{C_N, Y2, Q2, T2\}$, where $Pid_{\text{st}j} = E_{Mk}(\text{id}_{\text{st}j}, r_n)$, and the sizes of $\text{id}_{\text{st}j} = 64$ and $r_n = 32$ bits, so $Pid_{\text{st}j} = 96$ bits can be accommodated in one block. Similarly, $Q1 = E_{\text{ST}j}[\text{SM}_{\text{ID}j}, T1]$ is also of size 96 bits, and it needs one encryption block of size 128 bits. The total size of initial request message is $\{128 + 128 + 320 + 160 + 32\} = 768$ bits $= 96$ B. Likewise, the length of th reply message $\{C_N, Y2, Q2, T2\}$ is $\{320 + 160 + 256 + 32\} = 768$ bits $= 96$ B. Therefore, total communication cost of the proposed *LAS-SG* is $96 + 96 = 192$ B. The communication costs of the schemes of Kumar et al. [6], Chaudhry et al. [9], Kumar et al. [7], Odelu et al. [3], Tsai and Lu [5], Mahmood et al. [4], Garg et al. [8], and Khan et al. [10] are 272, 156, 148, 160, 180, 180, 156 and 392 B, respectively. The *LAS-SG* has slight extra communication cost, computed through comparisons with all schemes [3]–[5], [7]–[9] except with the schemes of Kumar et al. [6] and Khan et al. [10]. The performance comparisons of the *LAS-SG* and related schemes are given in Table IV.

C. Security Features

In this section, the attack resistance and security feature comparisons of our *LAS-SG* and related schemes [3]–[10] is presented. The comparisons are also given in Table V. The scheme of Mahmood et al. [4] is proved to be insecure against impersonation and ephemeral secret leakage attacks by Liang et al. [22]. Odelu et al. [5] argued that the scheme of Tasi and Lu [3] had weaknesses against ESLA. Moreover, Tasi and Lu [3] and Odelu et al. [5] schemes are insecure against impersonation, the man in middle and DoS attacks. The schemes of Kumar et al. [7] and Khan et al. [10] have faulty authentication phases and cannot extend session key among two entities of the SG environment as proved in [23] and [24], respectively. Due to the formation of the insecure certificate, the scheme presented in [9] is insecure against the physical capturing of an SM. As per the cryptanalysis conducted by Yahya et al. [26], the scheme of Kumar et al. [6] has insecurities against ESLA, stolen verifier, and traceability attacks. The analysis in [25] shows that the scheme of Garg et al. [8] is weak against key compromise impersonation attacks, and it lacks the required SM anonymity and perfect forward secrecy. The proposed scheme only resists known attacks and provides an adequate level of security render the *LAS-SG* best suitable to provide secure provision of services to an SM by the NAN gateway.

VI. Conclusion

This article presented a novel and ECC-based LAS-SG. The *LAS-SG* facilitates the formation of a secure channel among an SM and NAN gateway through sharing of a session key. The security of the *LAS-SG* is verified formally and through a discussion on the provision of security requirements of the proposed *LAS-SG*. The *LAS-SG* fulfills the known security requirements and resists known attacks, including key compromise impersonation attacks, along with the provision of communication and computation efficiencies as compared with the related schemes. Currently, the LAS-SG can extend a secure channel among a NAN gateway and SM, and in future, we intend to extend our scheme to provide end to end secure channel among all the entities of the SGI.

References

[1] N. Saxena and B. J. Choi, “State of the art authentication, access control, and secure integration in smart grid,” *Energies*, vol. 8, no. 10, pp. 11883–11915, 2015.

[2] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Perez-Gonzalez, “Privacy-preserving data aggregation in smart metering systems: An overview,” *IEEE Signal Process*, vol. 30, no. 2, pp. 75–86, Mar. 2013.

[3] J.-L. Tsai and N.-W. Lo, “Secure anonymous key distribution scheme for smart grid,” *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[4] K. Mahmood et al., “Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure,” *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, 2018.

[5] V. Odelu, A. K. Das, M. Wazid, and M. Conti, “Provably secure authenticated key agreement scheme for smart grid,” *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.

[6] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, “Lightweight authentication and key agreement for smart metering in smart energy networks,” *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 4349–4359, Jul. 2018.

[7] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, “Eccauth: A secure authentication protocol for demand response management in a smart grid system,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.

[8] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, “Secure and lightweight authentication scheme for smart metering infrastructure in smart grid,” *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3548–3557, May 2020.

[9] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, “Securing demand response management: A. certificate-based access control in smart grid edge computing infrastructure,” *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[10] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, “Palk: Password-based anonymous lightweight key agreement framework for smart grid,” *Int. J. Elect. Power Energy Syst.*, vol. 121, 2020, Art. no. 106121.

[11] B. LaMacchia, K. Lauter, and A. Mityagin, “Stronger security of authenticated key exchange,” in *Proc. Int. Conf. Provable Secur.*, 2007, pp. 1–16.

[12] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[13] R. Canetti and H. Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels,” in *Proc. Adv. Cryptol. - EUROCRYPT*, 2001, pp. 453–474.

[14] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, “A lightweight message authentication scheme for smart grid communications,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[15] D. H. et al., “An enhanced public key infrastructure to secure smart grid wireless communication networks,” *IEEE Netw.*, vol. 28, no. 1, pp. 10–16, Jan./Feb. 2014.

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

[17] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, “Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions,” in *Proc. IEEE 3rd Int Conf. Smart Grid Commun.*, 2012, pp. 324–329.

[18] S. Challa et al., “Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems,” *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, 2018.

[19] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, “Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems,” *Comput. Commun.*, vol. 153, pp. 527–537, 2020.

[20] K. Mahmood, J. Arshad, S. A. Chaudhry, and S. Kumari, “An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure,” *Int. J. Commun. Syst.*, vol. 32, no. 16, 2019, Art. no. e4137.

[21] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, “A novel identity-based key establishment method for advanced metering infrastructure in smart grid,” *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.

[22] X.-C. Liang, T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, and J.-H. Yeh, “Cryptanalysis of a pairing-based anonymous key agreement scheme for smart grid,” in *Proc. Adv. Intell. Inf. Hiding Multi. Signal Process*. 2020, pp. 125–131.

[23] S. A. Chaudhry, K. Yahya, and F. Al-Turjman, “Correctness of an authentication scheme for managing demand response in smart grid” Smart-Grid in IoT-Enabled Spaces: The Road to Intelligence in Power, p. 223, 2020.

[24] S. A. Chaudhry, “Correcting “palk: Password-based anonymous lightweight key agreement framework for smart grid”,” *Int. J. Elect. Power Energy Syst.*, vol. 125, 2021, Art. no. 106529.

[25] S. A. Chaudhry, J. Nebhen, K. Yahya, and F. Al-Turjman, “A privacy enhanced authentication scheme for securing smart grid infrastructure,” *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2021.3119685.

[26] K. Yahya, S. A. Chaudhry, and F. Al-Turjman, “On the security of an authentication scheme for smart metering infrastructure,” in *Proc. Emerg. Technol. Comput.*, 2020, pp. 1–6.

[27] M. Abdalla, P.-A. Fouque, and D. Pointcheval, “Password-based authenticated key exchange in the three-party setting,” in *Proc. Int. Workshop Public Key Cryptogr.*, 2005, pp. 65–84.

[28] D. He, S. Zeadally, N. Kumar, and W. Wu, “Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2052–2064, Sep. 2016.

[29] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, “A provably secure and anonymous message authentication scheme for smart grids,” *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, 2019.

[30] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, “Amassing the security: An ECC-based authentication scheme for Internet of Drones,” *IEEE Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Mar. 2021.