Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids

Vincent Omollo Nyangaresi[1(✉)], Zaid Ameen Abduljabbar[2,3], Salah H. Abbdal Refish[4], Mustafa A. Al Sibahee[5,6], Enas Wahab Abood[7], and Songfeng Lu[8,9]

[1] Faculty of Biological and Physical Sciences, Tom Mboya University College, Homabay, Kenya
vnyangaresi@tmuc.ac.ke
[2] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
zaid.ameen@uobasrah.edu.iq
[3] Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, China
[4] Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq
salah.hassan@sadiq.edu.iq
[5] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
mustafa@sztu.edu.cn
[6] Computer Technology Engineering Department, Iraq University College, Basrah, Iraq
[7] Department of Mathematics, College of Science, University of Basrah, Basrah, Iraq
enas.abood@uobasrah.edu.iq
[8] Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, China
lusongfeng@hust.edu.cn
[9] Shenzhen Institute of Huazhong University of Science and Technology, Shenzhen, China

Abstract. The security and privacy protection of smart grid data exchanged over the open and public wireless communication channels is critical yet challenging in this environment. Conventionally, public key cryptography, group signatures, blind signatures, identity based schemes and elliptic curve cryptography could provide the much needed security and privacy. However, all these techniques either lack some smart grid security requirements or have intensive communication, storage and computation overheads. This obviously renders them inefficient for resource-constrained smart grid network devices. In this paper, an anonymous key agreement and authentication protocol to address some of these challenges is proposed. The simulation results showed that the proposed protocol is the most efficient in terms of bandwidth and computation requirements. It also required relatively less memory space during its entire execution than some of the related protocols. Further, it is demonstrated that it

H. Jin et al. (Eds.): CROWNCOM 2021/WiCON 2021, LNICST 427, pp. 325–340, 2022.
https://doi.org/10.1007/978-3-030-98002-3_24

offers both backward and forward key secrecy, anonymity, and is robust against impersonation, session hijacking, privileged insider, side-channels, packet replays, packet injection and privacy leaks attacks.

Keywords: Ephemerals · Mutual authentication · Nonce · Privacy leaks · Security · Session keys · Smart grids

1 Introduction

The inability of the conventional power grid to accurately control power transmission from power generators to users owing to operation center's lack of real time electricity consumption report [1] has led to the deployment of smart grids. The smart grids ride on internet of things (IoT) and offer intelligent generation, transmission and distribution of electricity. In so doing, smart grids enhance flexibility, efficiency, reliability and quality of energy delivered by power networks [2]. As a typical Indus-trial Internet of Things (IIoT) category, these grid systems offer dynamic electric power consumption adjustments based on users' needs. However, since the communication between utility service providers (USPs) and smart meters (SMs) is over the open public wireless networks, the transmitted data is vulnerable to numerous security and privacy attacks [3]. The connection of power grids to cyber networks offers advanced control and monitoring at the expense of cyber attacks [4]. Authors in [5] identify Home area networks (HANs) as the most susceptible smart grid components owing to lack of direct control by utilities. Consequently, device authentication needs to be deployed to enhance the security of these networks.

Authors in [6] point out that poor protection of the smart grid network may lead to intrusions that can bring down the entire network. Although security plays a crucial role here, the conventional security goals of integrity, confidentiality and authentication are not enough in this environment. For instance, privacy of the electricity consumption report needs to be assured [7]. Although security is meant to ensure that entities authenticate themselves before any data exchange [8], data leakages in smart grids has surged [9]. Since these real-time power consumption reports are associated with users' privacy such as economic status and lifestyle, robust protection is required. Authors in [10] have identified mutual authentication before the transmission of any sensitive data as being key for trusting identities within the smart grid. Through this authentication, the SMs and USPs verify each others' identity after which they negotiate a secret session key for data protection over insecure channels [10].

Unfortunately, authentication protocols based on the conventional public-key infrastructure (PKI) are computationally intensive and hence not ideal for resource constrained smart grid systems and other IoT devices within this network [11]. Schemes based on certificate authority (CA) that issue certificates to devices exhibit high communication costs. Although the current identity based approaches eliminate certificate management problems, the real identities of the communicating entities must be revealed during verification. Ring signatures and blind signatures can address the identity leakage problem [12] but these signatures render the tracing of smart grid malicious entities very cumbersome. In addition, they incur high computation and

communication overheads [13]. Although group signature based authentication address this traceability problem, it has high computation and communication over-heads.

It is evident that despite the development of many authentication schemes for the smart grid environment, robust security and privacy protection still present some challenges [14]. As authors in [15] point out, although the current cryptographic protocols were designed to enable secure communication over the smart grid network, most of them do not offer flexible key management and anonymity. As such, the identified security, performance and privacy issues need to be addressed. The contributions of this paper are as follows:

I. We develop a protocol based on pseudo-identities for both smart meter and utility service provider so as to offer strong anonymity
II. The session keys are dynamically derived from random nonces for every authentication process to preserve backward and forward key secrecy
III. The stored user specific parameters are XOR-masked followed by one way hashing operations to thwart side-channel attacks.
IV. Using both Dolev–Yao and Canetti-Krawczyk models, we show that the proposed protocol offers protection from typical smart grid attacks such as message injection and replays.

The rest of this paper is organized as follows: Sect. 2 presents a discussion on related work while Sect. 3 elaborates on the deployed system model. On the other hand, Sect. 4 presents simulations results together with evaluations of the developed protocol. Finally, Sect. 5 concludes this paper and gives future direction in this research domain.

2 Related Work

Smart grid security and privacy has attracted much interest in both industry and academia, leading to the development of many schemes. For instance, authors in [16] develop a scheme for session negotiation but its bilinear pairing operations led to high computational costs. Elliptic curve cryptography (ECC) based identity-based key establishment protocol has been presented in [17] for smart grids but which resulted to high computation overheads at the SM side. In addition, the schemes in [16] and [17] fail to offer privacy protection during the key agreement and authentication process. Authors in [18] proposed a scheme which transmitted the SM real identity over the insecure channels and hence compromised SM anonymity. Therefore, the authors in [19] introduced an anonymous key agreement protocol, but which never offered mutual authentication since the SM does not validate the utility control. An efficient identity-based anonymous authentication scheme has been presented in [20], which fails to consider key management of communicating entities. On the other hand, a key management and authentication protocol in [21] does not provide device anonymity and revocation.

A protocol for conditional anonymity and dynamic participation using group and blind signatures was presented in [22] while authors in [23] have introduced a privacy preserving technique using group signatures. In addition, attribute certificates and ring

signature based privacy protection approach has been presented in [24]. However, the schemes in [22–24] are computationally intensive due to the usage of group and rings signatures. On the other hand, a key distribution scheme has been presented in [25], but which is vulnerable to secret leakage attacks and does not offer session key security. ECC based key establishment protocol has been developed in [26] while authors in [27] have proposed a novel device authentication protocol. However, both schemes in [26] and [27]employ PKI which is computationally intensive for smart grid devices.

The protocol developed in [28] for smart grid key management is susceptible to man-in-the-middle (MitM) attacks while the scheme presented in [29] for secure key distribution is susceptible to impersonation attacks. Authors in [30] have presented a bilinear pairings based mutual authentication protocol in the smart grid environment but which is vulnerable to tracking and impersonation attacks. An authentication scheme based on bilinear maps was developed in [31] to address these issues, but it has high computational overheads. On their part, authors in [32] presented an ECC based scheme for SM anonymity, but which is still susceptible to ephemeral secret key leakages. A three-factor user authentication protocol has been presented in [33], which fails to offer flexible revocation of malicious SMs.

The anonymous authentication and key agreement approach in [34] employs time-stamps, which renders it vulnerable to de-synchronization attacks and the neighborhood area network gateway (NANG) need to store numerous symmetric keys for various HANs gateways. Authors in [35] present ECC based privacy protection protocol, which experienced low computation costs while authors in [36] have developed ECC-based authentication protocol, which does not offer secure mutual authentication and is still vulnerable to impersonation and session key disclosure attacks. Moreover, the protocols in [25] and [30] fail to achieve smart grid security requirements while the techniques in [31–33] and [35] are computationally intensive due to elliptic curve point multiplication operations. Consequently, privacy protection under low computation operations during authentication process still remains challenging.

3 System Model

The current smart grid authentication and key agreement protocols have been observed to be susceptible to numerous security, performance and privacy challenges. Lack of anonymity and untraceability are some of the SM security requirements not considered in most of these protocols. In terms of performance, PKI based techniques have been observed to be computationally intensive. Although ECC based techniques offer anonymous authentication and key agreement at lower computation costs than PKI based approaches, most of these schemes incorporate bilinear pairing operations which are time-consuming. Consequently, the attainment of robust security and privacy in a smart grid environment at lower communication and computation costs still presents some challenges. As such, we propose a lightweight key agreement and authentication protocol based on only pseudo-identities, ephemerals, XOR and hashing operations. For these operations, the following definitions hold:

Definition 1: For a secure hash function $h(.)$: (a) given input message z of arbitrary length, the message digest of fixed length output h(z) can be generated (b) given y, it is cumbersome to compute $z = h^{-1}(y)$ (c) given z, it is computationally infeasible to find $z' \neq z$ such that $h(z') = h(z)$.

Definition 2: In the Dolev–Yao model, adversary $\mathcal{O}$: (a) can be valid but malicious user (b) is able to control the open communication medium hence can modify, intercept, insert or erase transmitted messages (c) can obtain secrets stored in the smart device (SD) upon successful access of the SD through side-channel attacks (d) is a probabilistic polynomial time adversary and hence can guess low entropy passwords and other identity data within polynomial time (e) can physically capture and extract sensitive data stored in any smart meter within a smart grid since they are not tamper proof (f) cannot compromise the registration authority since it is fully trusted.

Definition 3: In the Canetti and Krawczyk's (CK) adversary model, adversary $\mathcal{O}$ has all Dolev–Yao model capabilities, and in addition is able to compromise ephemeral information such as session-specific states and keys.

Definition 4: Based on the one-time pad theorem, any value *XORed* with a random value yields a random output.

As illustrated in Fig. 1, the smart grid network model consists of three entities communicating over the insecure internet. The smart meter (SM) and the utility service provider (USP) communicate with each other via the Trusted Authority (TA), where the two first register before they are issued with security tokens to enable them mutually authenticate each other and establish a session key.

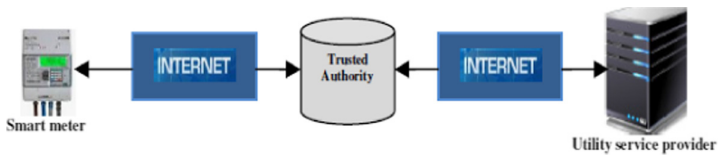

Fig. 1. Smart grid-utility service provider model

Since the exchanged power consumption reports are over the public internet, the security features pursued in this paper include anonymity, untraceability, mutual authentication, session key security, backward and forward secrecy and robustness against impersonation, side-channel, packet replay, session hijack, privileged insider, and packet injection attacks. Table 1 gives the notations used in this paper and their brief descriptions.

Table 1. Notations

Notation	Description
ɖ	USP center pseudo-identity
ƙ	SM pseudo-identity
η_i, $\bar{Q}_i$, ɾ, C'	Nonces
Φ	TA's master key
ß, ƀ, Б	SM authentication request messages
ƥ, ƚ, ɠ	USP authentication messages
Z	Session key
⊕	XOR operator
‖	Concatenation operator

The proposed protocol comprised of three major phases which included parameter setting, registration and mutual authentication.

Parameter Setting and Registration: During these phases, the TA registers both the SM and USP upon which unique pseudo-identities $ƙ$ and $ɖ$ are assigned to each of them (step 1). Afterwards, the TA buffers these parameters in the respective devices. As shown in Fig. 2, for the SM to receive power management services from the USP, the TA generates nonces η and $\bar{Q}$ for it (step 2) before computing security parameters R, ψ, $ƪ$ and $Ħ$ (step 3) for subsequent authentication. Then, the TA stores $\{\eta, R\}$ in its repository before transmitting $\{ƪ, Ħ, \bar{Q}\}$ to the SM (step 4). Upon receipt of these parameters, SM computes security parameter $ƛ$ (step 5) and buffers the security set $\{ƪ, Ħ, ƛ\}$ for subsequent authentication. Similarly, the USP's attempt to offer power management services to the SM triggers the TA to retrieve security set $\{R, \eta\}$ from its memory to calculate security tokens $ȝ$ and ψ (step 6) before sending the set $\{ȝ, R\}$ to the USP (step 7). Afterwards, the USP calculates security tokens $ς$ (step 8) before buffering security tokens $\{ȝ, R\}$. This marks the end parameter setting and device registration and the onset of mutual authentication as shown in Fig. 3.

INPUT: ƙ, ɖ, η, $\bar{Q}$
OUTPUT: R, ψ, ƪ, Ħ, ƛ, ȝ, ς

BEGIN:
1.) Generates pseudo-identities ƙ & ɖ /* *Parameter setting* */
2.) Generate SM nonces η & $\bar{Q}$ /* *Onset of device registration* */
3.) Compute R=h(ƙ||$\bar{Q}$), ψ=h(R||Φ||η), ƪ= ψ⊕hR||$\bar{Q}$), Ħ=h(R||ψ)
4.) TA→SM: {ƪ, Ħ, $\bar{Q}$}
5.) Compute ƛ=h(ƙ||Ħ)⊕$\bar{Q}$
6.) Retrieve {R,η}, calculate ȝ=h(ɖ||Φ) & ψ=h(R||Φ||η)
7.) TA→USP: {ȝ, R}
8.) Compute ς= ψ⊕ɖ /* *end of device registration* */
END

Fig. 2. Parameter setting and device registration

SM-USP Mutual Authentication: The authentication session is initiated by having the SM compute security tokens $\bar{Q}$, R, ψ and H^* (step 1). Then security token H^* is validated against H such that if they are not similar, the authentication is aborted (step 2). However, if they are similar, then the SM proceeds to generate nonce r_s before deriving authentication messages $\{\beta, b, B\}$ (step 3).

INPUT: r_s, C', k, d_s, λ, H, y, R, ς
OUTPUT: $\bar{Q}$, ψ, H^*, β, b, B, β, γ, Z, g, r_s^*, R^*, B^*, C'^*, γ^*, Z^*, g^*

BEGIN:
1. Compute $\bar{Q}=\lambda \oplus h(k||H)$, $R=h(k||\bar{Q})$, $\psi=y \oplus h(R||\bar{Q})$, $H^*=h(R||\psi)$
2.) **IF** $H^*!=H$ **THEN:**
Abort authentication
3.) **ELSE:**
Generate nonce r_s and compute $\beta= \psi \oplus r_s$, $b= R \oplus h(\psi||r_s)$, $B=h(R||\psi||r_s)$
4.) SM→USP: $\{\beta, b, B\}$
5.) Retrieve $\{\varsigma, R\}$ and compute $\psi= \varsigma \oplus d_s$, $r_s^*= \beta \oplus \psi$ & $R^*=b \oplus h(\psi||r_s)$
6.) **IF** $R^*!=R$ **THEN**:
Abort authentication
7.) **ELSE**:
Calculate $B^*=h(R^*||\psi||r_s^*)$
8.) **IF** $B^*!=B$ **THEN:**
Abort authentication
9.) **ELSE:**
Generate nonce C' and calculate $\beta= C' \oplus h(\psi||C')$, $\gamma=\gamma \oplus C'$, $Z=h(r_s||C')$, $g=h(R||\psi||r_s||C')$
10.) USP→ SM: $\{\beta, \gamma, g\}$
11.) Compute $C'^*= \beta \oplus h(\psi||C')$, $\gamma^*= \gamma \oplus C'$, $Z^*=h(r_s||C')$, $g^*=h(R||\psi||r_s||C')$
12.) **IF** $g^*!=g$ **THEN:**
Abort authentication
13.) **ELSE:**
Trust SM and initiate packet exchange
14. **ENDIF**
15. **ENDIF**
16. **ENDIF**
17. **ENDIF**
END

Fig. 3. SM-USP mutual authentication

This is followed by the transmission of authentication request message triplet $\{\beta, b, B\}$ to the USP (step 4). Upon receipt of this triplet, the USP retrieves tokens $\{\varsigma, R\}$ from its buffer to re-compute ψ, r_s^*, and R^* (step 5) before validating R^* against R. If these two security parameters are dissimilar, authentication is aborted (step 6), otherwise token B^* is re-computed (step 7) and validated against B such that is they are dissimilar, the authentication session is aborted (step 8).

However, if the two are similar, the USP proceeds with the generation of nonce C' for the computation of security parameters triplet $\{\beta, \gamma, g\}$ in step 9. In step 10, authentication messages triplet $\{\beta, \gamma, g\}$ is transmitted to the SM. Upon receiving this triplet, the SM re-computes C'^*, γ^*, Z^* and g^* (step 11) before validating g^* against g such that if they are dissimilar, authentication is aborted (step 12). However, if they are similar, the SM and USP can trust one another and commence packet exchanges. Figure 4 presents the message flow in the proposed protocol.

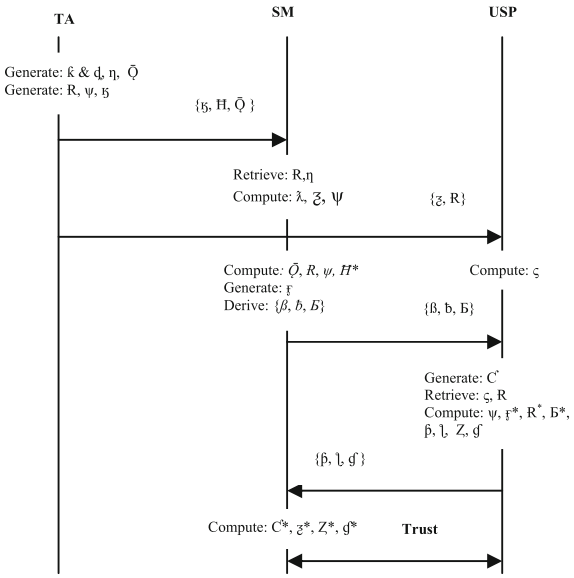

Fig. 4. Proposed message exchanges

As shown in Fig. 4, the TA controls the registration phase of both the SM and USP. After this registration, the SM and USP exchange a number of authentication messages. At the end of the successful mutual authentication process, some trust level is established between the SM and USP and hence they can commence payload exchanges.

4 Results and Discussion

The proposed protocol was simulated using NS2 2.35 network simulator running on Ubuntu 14.04 LTS platform. The simulation environment consisted of smart meters, the utility service provider and trusted authority. Table 2 presents the parameters that were deployed during the simulation process.

Table 2. Simulation parameters

Parameter	Description
Maximum number of SMs	50
Maximum SM transmission range	100 m
Number of USPs	1
Number of TAs	1
MAC protocol	IEEE 802.11
Platform	Ubuntu 14.04 LTS
Routing protocol	DSDV
Simulation duration	2000 s

As shown in Table 2, the maximum number of smart meter devices was 50 with each of them having a maximum transmission range of 100 m. On the other hand, there was only one utility service provider and one trusted authority. The media access control layer protocol was IEEE 802.11 while the routing protocol was Destination-Sequenced Distance Vector (DSDV). The simulations were executed for the duration of 2000 s.

In this section, performance of the proposed protocol is evaluated using communication overheads, computation overheads and space complexity. On the other hand, the security of the proposed protocol is evaluated using both Dolev–Yao (DY) and Canetti- Krawczyk (CK) models, which are widely utilized to prove the features of interactive cryptographic protocols. Section 4.1 describes the security analysis of the proposed protocol while Sect. 4.2 discusses the performance evaluation of this protocol.

4.1 Security Analysis

In both DY and CK models, network communications are assumed to occur over insecure channels and none of the communicating entity is trustable. Under adversarial properties in Definitions 2 and 3, the proposed protocol was evaluated against impersonation, side-channel, packet replays, packet injection and privacy leaks attacks as illustrated below. These attack models fairly represented all the assumptions of both DY and CK security evaluation models.

Impersonation Attacks: in this attack, it is assumed that an adversary is capable of physically capturing the smart meter and eavesdropping all the transmitted packets. For any successful impersonation, an attacker must generate valid authentication requests $\{\beta, \hbar, Б\}$ and receive valid authentication responses $\{\rho, \wr, g\}$. However, the computation of these messages incorporates random nonces $\mathfrak{F}$ and C, which are infeasible to guess correctly. Moreover, an attacker does not possess secret parameter ψ nor is the correct computation of session key Z possible due to the one way-hashing operation of the random nonces.

Side-Channel Attacks: suppose that an attacker has physical access to the smart meter and is able to extract a set of secrets $\{\flat, \mathit{H}, \lambda\}$ stored in its memory. Due to the usage of XOR masking followed by one way hashing operation, user specific security parameters $\{\kappa, \bar{Q}, \psi\}$ cannot be obtained from the memory extracted contents.

Packet Replay Attacks: in the proposed protocol, the freshness of transmitted messages is validated using $\{Б, Б^*, g, g^*\}$. Consequently, an attacker is unable to resend previously sent messages due to frequent updating of all sent messages for every authentication session.

Session Hijack Attacks: suppose that an adversary attempts to compute session key Z to facilitate this attack. Any such successful session computation requires correct calculation of a set of authentication messages $\{\beta, \hbar, Б\}$. However, these authentication messages incorporate random nonce $\mathfrak{F}$ and secret security parameter ψ which are unavailable to the attacker nor can they be computed accurately due to their stochastic nature. As such, this attack will fail.

Privileged Insider Attacks: in this attack, it is assumed that some entity at the USP is able to retrieve a set of parameters $\{R, \mathcal{Z}, \varsigma\}$ needed to authenticate the smart meter. However, since these parameters cannot yield specific smart meter pseudo-identity κ and security parameter ψ, this attack fails. This is because the set $\{\kappa, \psi\}$ can only be computed using correct nonce $\mathfrak{x}$ and q, which are unavailable to the privileges insider entity.

Packet Injection Attacks: the aim of this attack is to interrupt successful mutual authentication between the smart meter and the USP through the injection of bogus packets. However, upon receipt of authentication request message set $\{\beta, \mathfrak{b}, \mathcal{B}\}$ from the smart meter, the USP validates message $\mathcal{B}^*$ using $\mathcal{B}$. In addition, the smart meter also validates the USP upon receipt of $\{\mathcal{p}, \mathfrak{l}, g\}$ using g^* and g. It is after the successful authentication that any messages can be exchanged between the SM and USP and hence this attack will fail.

Privacy Leaks Attacks: in the proposed protocol, the entire authentication process makes use of pseudo-identities for both the smart meter and USP which are further masked through XOR operations before being hashed. As such, it is infeasible for attackers to capture the real identities of the SM or USP.

The security features of proposed protocol are then compared with those of the schemes in [25, 30] and [36] as shown in Table 3.

Table 3. Security features comparisons

Security feature	[25]	[30]	[36]	Proposed
Impersonation	Yes	Yes	No	Yes
Packet replays	Yes	Yes	No	Yes
Privileged insider	No	Yes	Yes	Yes
MitM	Yes	Yes	Yes	Yes
Session hijacking	No	Yes	No	Yes
Privacy leaks	Yes	Yes	Yes	Yes
Forward key secrecy	Yes	Yes	Yes	Yes
DoS protection	No	No	Yes	Yes

Based on Table 3, it is evident that the proposed protocol offers all the security features followed by the protocol in [30] which lacked protection against DoS. On the other hand, the schemes in [25] and [36] lacked three security features each.

4.2 Performance Evaluation

The initial simulations that were executed encompassed the analysis of the end-to-end (E2E) latencies and throughput of the proposed protocol. Thereafter, the size of the exchanged messages, the time it took to compute the security tokens needed for session key agreement and mutual authentication, and the memory storage space required for the full execution of the proposed protocol are compared with other related schemes.

E2E: to analyze the E2E delay characteristics of the proposed protocol, the average time taken to route packets from the source to the destination was measured for different SMs densities as shown in Fig. 5 (a) below. It is evident that there is a general increase in E2E delays as the number of smart meters were increased from an initial value of 1 to a maximum value of 50. This is attributed to the surging number of messages exchanged among the TA, SM and USP for high SMs densities. As such, congestion crops in within the network which causes some processing delays at the endpoints.

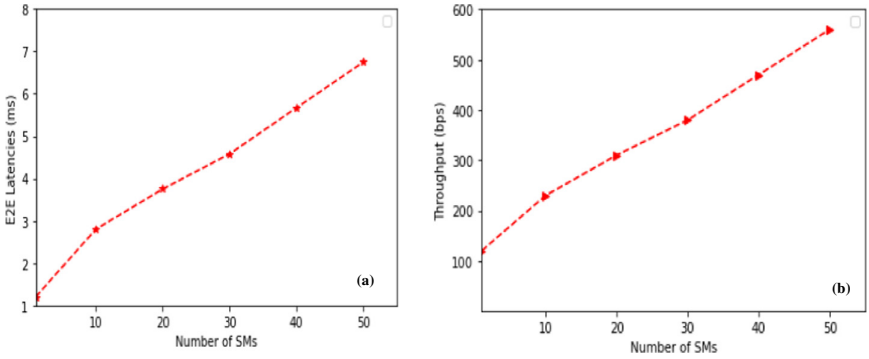

Fig. 5. (a) E2E variations (b) Throughput variations

Throughput: to determine the throughput of the proposed protocol, the number of bits conveyed within the network per unit time was measured. To accomplish this, the number of smart meters was increased from 1 to a maximum of 50 as the number of bits transferred was measured. The results obtained are shown in Fig. 5 (b), from which it can be seen that as the number of smart meters in the network increases, there is a corresponding increase in the network throughput. This is because the surge in the number of smart meters implies an increase in the number of exchanged packets within the network. As such, the network throughput for 50 smart meters was higher compared with the throughput for a single smart meter.

Computation Costs: based on values in [37], during mutual authentication, ECC point multiplication T_m, ECC point addition T_a, hashing T_h, bilinear operation T_b, exponentiation T_e, and symmetric encryption or decryption $T_{e/d}$ operations are normally executed, which take 2.226 ms, 0.0288 ms, 0.0023 ms, 5.811 ms, 3.85 ms, 0.0046 ms respectively. However, considering Fig. 2 and Fig. 3, the proposed protocol executed only 16 one way hashing operations and therefore its cumulative computation cost is 0.0368 ms as shown in Table 4.

Table 4. Computation costs comparisons

Protocol	Computation costs (ms)
[25]	30.4796
[30]	34.9273
[36]	8.9316
Proposed	0.0368

On the other hand, the schemes in [25, 30] and [36] take 30.4796 ms, 34.9273 ms and 8.9316 ms respectively. It is evident that our protocol had the least computation costs owing to its lightweight XOR and hashing operations. On the other hand, the scheme in [25] required $5T_m$, $2T_e$, $2T_b$, and $12T_h$ operations while the protocol in [30] needs $7T_m$, $2T_e$, $2T_b$, and $10T_h$ operations. On the other hand, the scheme in [36] requires only $4T_m$ and 12 T_h operations.

Communication Costs: many of the exchanged parameters during authentication include device identities, timestamps, hashes, random nonces and ECC cryptosystem parameters whose sizes are 160 bits, 32 bits, 160 bits, 160 bits and 320 bits respectively. In the proposed protocol, the messages exchanged during the mutual authentication process included $\{\beta, \hbar, E\}$ and $\{\beta, \ell, g\}$ which required 480 bits. This value was then compared with those of the schemes in [25, 30] and [36] as shown in Table 5.

Table 5. Communication costs comparisons

Protocol	Communication costs (bits)
[25]	1408
[30]	1920
[36]	1376
Proposed	480

It is evident from Table 5 that the schemes in [25, 30] and [36] require 1408 bits, 1920 bits and 1376 bits respectively. These values were very high compared with the exchanged bits in the proposed protocol, as evidenced in Fig. 6.

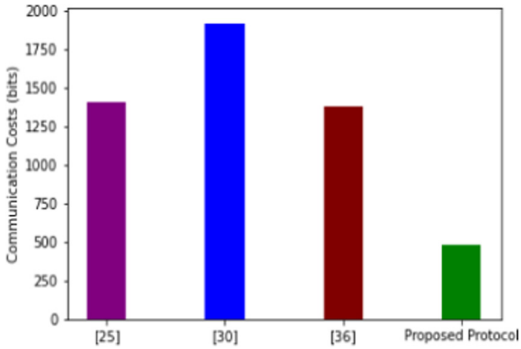

Fig. 6. Communication costs comparisons

In the proposed protocol, only two sets of messages were exchanged between the USP and SM during the authentication process. However, all these other schemes required three sets of messages to be exchanged. As such, our protocol is the most efficient in terms of bandwidth requirements.

Space complexity: a typical authentication protocol needs to store the public key cryptosystem parameters, random nonces, timestamps, hashes and device identity, which occupy 40 bytes, 20 bytes, 4 bytes, 20 bytes and 20 bytes respectively. In the proposed protocol, only message sets $\{\mathcal{b}, \mathcal{H}, \mathcal{\lambda}\}$ and $\{R, \mathcal{z}, \psi\}$ required storage at the SM and USP respectively. Here, the storage requirements for $\mathcal{b} = \mathcal{H} = \mathcal{\lambda} = 20$ byes hence the total space complexity for $\{\mathcal{b}, \mathcal{H}, \mathcal{\lambda}\}$ is 60 bytes. Similarly, $R = \mathcal{z} = \psi = 20$ bytes and hence message $\{R, \mathcal{z}, \psi\}$ requires 60 bytes. Consequently, the cumulative storage requirement for the proposed protocol is 120 bytes as shown in Table 6.

Table 6. Space complexity comparisons

Protocol	Storage costs (bytes)		
	SM	USP	Cumulative
[25]	40	40	80
[30]	80	80	160
[36]	40	40	80
Proposed	60	60	120

On the other hand, the scheme in [25] required 40 bytes at the SM and 40 bytes at the USP, the scheme in [30] needed 80 bytes on the SM and 80 bytes on the USP while the protocol in [36] required 40 bytes on both the SM and USP. As such, the space complexities for protocols in [25, 30] and [36] are 80 bytes, 160 bytes and 80 bytes respectively, as shown in Fig. 7.

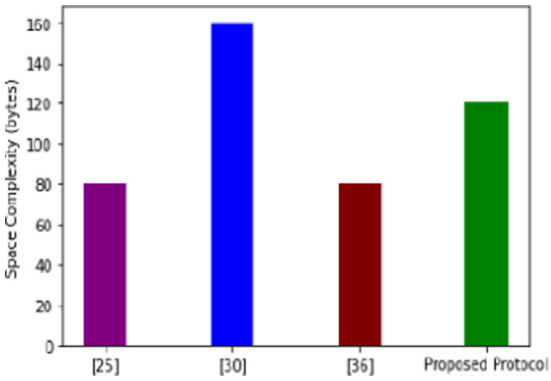

Fig. 7. Space complexity comparisons

Based on the graphs in Fig. 7, the proposed protocol had slightly higher space storage requirements than protocols in [25] and [36]. Although our scheme had higher space complexities than these schemes, it offers superior security features as shown in Table 3 above.

5 Conclusion and Future Work

Smart grid privacy and security has been noted to be challenging owing to the resource constrained nature of smart grid components. The bilinear pairing operations and elliptic curve point multiplication operations in ECC, certificate distribution and maintenance of revocation lists in PKI, signature signing and verification are all intensive in terms of the exchanged messages and the processing time involved. On the other hand, identity based schemes leads to the revelation of smart grid entities' real identities to the verifiers during authentication. Consequently, deploying conventional ECC, PKI, signature, and identity based schemes results in high communication and computation overheads or privacy leaks. The proposed protocol mutually authenticated the smart meters to the USP at lower communication and computation costs. It also required relatively low storage costs and was demonstrated to be robust against many of the conventional smart grid security and privacy attacks. Future work lies in the formal verification of the security features of this protocol and its evaluation using other metrics that were not within the scope of this paper.

References

1. Song, J., Liu, Y., Shao, J., Tang, C.: A dynamic membership data aggregation (DMDA) protocol for smart grid. IEEE Syst. J. **14**(1), 900–908 (2019)
2. Lyu, L., Nandakumar, K., Rubinstein, B.I.P., Jin, J., Bedo, J., Palaniswami, M.: PPFA: privacy preserving fog-enabled aggregation in smart grid. IEEE Trans. Ind. Inform. **14**(8), 3733–3744 (2018)
3. Shrestha, M., Johansen, C., Noll, J., Roverso, D.: A methodology for security classification applied to smart grid infrastructures. Int. J. Crit. Infrastruct. Prot. **28**, 100342 (2020)
4. Liang, G., Weller, S., Zhao, J., Luo, F., Dong, Z.: The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans. Power Syst. **32**, 3317–3318 (2017)
5. Xiang, A., Zheng, J.: A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks. Electronics **9**(6), 989 (2020)
6. McDaniel, P., McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Secur. Priv. **7**(3), 75–77 (2009)
7. Liu, Y.-N., Wang, Y.-P., Wang, X.-F., Xia, Z., Xu, J.-F.: Privacy preserving raw data collection without a trusted authority for IoT. Comput. Netw. **148**, 340–348 (2019)
8. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: Neuro-fuzzy based handover authentication protocol for ultra dense 5G networks. In: 2020 2nd Global Power, Energy and Communication Conference (GPECOM), pp. 339–344. IEEE (2020)
9. Kalogridis, G., Efthymiou, C., Denic, S.Z., Lewis, T.A., Cepeda, R.: Privacy for smart meters: towards undetectable appliance load signatures. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communincation, pp. 232–237 (2010)
10. Wu, L., Wang, J., Choo, K.R., He, D.: Secure key agreement and key protection for mobile device user authentication. IEEE Trans. Inform. Forensics Secur. **14**(2), 319–330 (2019)
11. Nyangaresi, V.O., Rodrigues, A.J., Taha, N.K.: Mutual authentication protocol for secure VANET data exchanges. In: Perakovic, D., Knapcikova, L. (eds.) FABULOUS 2021. LNICSSITE, vol. 382, pp. 58–76. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-78459-1_5

12. Gong, Y., Cai, Y., Guo, Y., Fang, Y.: A privacy-preserving scheme for incentive-based demand response in the smart grid. IEEE Trans. Smart Grid **7**(3), 1304–1313 (2016)
13. Guan, Z., et al.: Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Commun. Mag. **56**(7), 82–88 (2018)
14. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: Efficient group authentication protocol for secure 5G enabled vehicular communications. In: 2020 16th International Computer Engineering Conference (ICENCO), pp. 25–30. IEEE (2020)
15. Wang, J., Wu, L., Choo, K.K.R., He, D.: Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Trans. Ind. Inf. **16**(3), 1984–1992 (2019)
16. Wan, Z., Wang, G., Yang, Y., Shi, S.: SKM: scalable key management for advanced metering infrastructure in smart grids. IEEE Trans. Ind. Electron. **61**(12), 7055–7066 (2014)
17. Mohammadali, A., Haghighi, M., Tadayon, M., Nodooshan, A.: A novel identity-based key establishment method for advanced metering infrastructure in smart grid. IEEE Trans. Smart Grid **9**(4), 2834–2842 (2018)
18. Mahmood, K., Chaudhry, S.A., Naqvi, H., Kumari, S., Li, X., Sangaiah, A.K.: An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. Future Gener. Comput. Syst. **81**, 557–565 (2018)
19. Mahmood, K., et al.: Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure. Future Gener. Comput. Syst. **88**, 491–500 (2018)
20. Jia, X., He, D., Kumar, N., Choo, K.K.R.: A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing. IEEE Syst. J. **14**(1), 560–657 (2019)
21. Kahvazadeh, S., Masip-Bruin, X., Diaz, R., Marín-Tordera, E., Jurnet, A., Garcia, J.: Towards an efficient key management and authentication strategy for combined fog-to-cloud continuum systems. In: 3rd Cloudification of the Internet of Things, CIoT 2018, Paris, France, pp. 1–7 (2018)
22. Zheng, H., Wu, Q., Qin, B., Zhong, L., He, S., Liu, J.: Linkable group signature for auditing anonymous communication. In: Susilo, W., Yang, G. (eds.) Information Security and Privacy, ACISP 2018. LNCS, vol. 10946, pp. 304–321. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93638-3_18
23. Ma, L., Liu, X., Pei, Q., Xiang, Y.: Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. IEEE Trans. Serv. Comput. **12**(5), 786–799 (2018)
24. Zhao, J., Liu, J., Qin, Z., Ren, K.: Privacy protection scheme based on remote anonymous attestation for trusted smart meters. IEEE Trans. Smart Grid **9**(4), 3313–3320 (2018)
25. Tsai, J.L., Lo, N.W.: Secure anonymous key distribution scheme for smart grid. IEEE Trans. Smart Grid **7**(2), 906–914 (2016)
26. Li, Y.: Design of a key establishment protocol for smart home energy management system. In: Proceedings of the 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, Madrid, Spain, pp. 88–93 (2013)
27. Vaidya, B., Makrakis, D., Mouftah, H.T.: Device authentication mechanism for smart energy home area networks. In: Proceedings of the 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 787–788 (2011)
28. Wu, D., Zhou, C.: Fault-tolerant and scalable key management for smart grid. IEEE Trans. Smart Grid **2**(2), 375–381 (2011)
29. Xia, J., Wang, Y.: Secure key distribution for the smart grid. IEEE Trans. Smart Grid **3**(3), 1437–1443 (2012)
30. Odelu, V., Das, A.K., Wazid, M., Conti, M.: Provably secure authenticated key agreement scheme for smart grid. IEEE Trans. Smart Grid **9**(3), 1900–1910 (2018)

31. Chen, Y., Martínez, J., Castillejo, P., López, L.: An anonymous authentication and key establish scheme for smart grid: FAuth. Energies **10**(9), 1–23 (2017)
32. He, D., Wang, H., Khurram Khan, M., Wang, L.: Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun. **10**(14), 1795–1802 (2016)
33. Wazid, M., Das, A.K., Kumar, N., Rodrigues, J.J.P.C.: Secure three-factor user authentication scheme for renewable-energy based smart grid environment. IEEE Trans. Ind. Inform. 13(6), 3144–3153 (2017)
34. Kumar, P., Gurtov, A., Sain, M., Martin, A., Ha, P.: Lightweight authentication and key agreement for smart metering in smart energy networks. IEEE Trans. Smart Grid **10**, 1–11 (2018)
35. Abbasinezhad-Mood, D., Nikooghadam, M.: An anonymous ECC-based self certified key distribution scheme for the smart grid. IEEE Trans. Ind. Electron. **65**(10), 7996–8004 (2018)
36. Kumar, N., Aujla, G.S., Das, A.K., Conti, M.: ECCAuth: a secure authentication protocol for demand response management in a smart grid system. IEEE Trans. Ind. Inform. **15**(12), 6572–6582 (2019)
37. Kilinc, H.H., Yanik, T.: A survey of SIP authentication and key agreement schemes. IEEE Commun. Surv. Tutor. **16**(2), 1005–1023 (2014)