Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids

Vincent Omollo Nyangaresi[1(✉)], Zaid Ameen Abduljabbar[2,3], Mustafa A. Al Sibahee[4,5], Enas Wahab Abood[6], and Iman Qays Abduljaleel[7]

[1] Faculty of Biological & 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] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
mustafa@sztu.edu.cn
[5] Computer Technology Engineering Department, Iraq University College, Basrah, Iraq
[6] Department of Mathematics, College of Science, University of Basrah, Basrah, Iraq
enas.abood@uobasrah.edu.iq
[7] Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq
iman.abduljaleel@uobasrah.edu.iq

Abstract. Smart grid networks offer two-way communication between the smart meters and the utility service providers (USPs). This enables the USPs to analyze real-time data emanating from the consumers and offer dynamic adjustments to the power generation and transmission. However, the periodical transmission of consumption reports from the smart meters towards the USPs over public channels exposes the exchanged messages to attacks such as eavesdropping, modification and bogus injections. Consequently, the power adjustments executed may not be occasioned by consumer requirements but by malicious entities within the smart grid network. To curb this, numerous schemes have been presented in literature. However, majority of these protocols are either susceptible to attacks or are inefficient. In this paper, a dynamic ephemeral and session key generation protocol is presented. The security analysis shows that if offers entity anonymity, mutual authentication, forward key secrecy and untraceability. In addition, it is shown to be resilient against typical smart grid attacks such as offline password guessing, denial of service (DoS), packet replays, privileged insider, man-in-the-middle (MitM), impersonation and physical capture. In terms of performance, it has the least execution times and bandwidth requirements among other related protocols.

Keywords: Attacks · Authentication · Privacy · Protocols · Security · Smart grids · Smart meters

W. Bao et al. (Eds.): ADHOCNETS 2021/TridentCom 2021, LNICST 428, pp. 188–204, 2022.
https://doi.org/10.1007/978-3-030-98005-4_14

1 Introduction

The Smart Grid (SG) is envisioned as the next-generation intelligent network that introduces efficiency in the delivery, management and integration of renewable and green energy technologies [1]. The SG basically provides a two-way information and energy exchange between the smart meter (SM) and the utility service provider (USP) [2]. A typical SG consists of control centers, communication modules and smart devices such as smart meters. In the SG networks, the SMs monitor power consumptions and stability of the supplied power [3]. In essence, the SM utilizes the two-way communication channel between the consumer and the USP to manage, exchange and control energy delivery and consumption at the customer premises [4]. Despite the offered convenience, the SMs raise security and privacy issues regarding the transmission of energy consumptions reports over the public networks [4, 5].

As explained in [6], the SG is one of the many application domains of Internet of Things (IoT) that utilizes the Internet Protocol (IP) for the exchange of information between the USP and the SMs. Through the bi-directional communication procedures, energy efficiency is realized [7] through dynamic adjustments to the power transmitted. Compared with the conventional power grids, SGs offer enhanced efficiency, reliability and sustainability [8]. However, many security issues such as Distributed Denial of Service (DDoS) lurk in the SG networks targeting the SMs and other SG components. In addition, other attacks inherent in conventional public channels [9] are also possible in SG networks.

In most application domains, the SMs are installed outside in an open environment within a home. This exposes the SMs to numerous attacks, including physical capture [4, 10] which may facilitate side-channel attacks through power analysis. According to [6], the communication module that interlinks different components introduces security vulnerabilities into the SG as a result of increased complexity and increased surfaces from where attacks can be launched against the electrical power system. As such, although the SG facilitates automated measurement and visualization of power consumptions, spoofing attacks are common in this environment [11]. The requirement that SMs transmit periodical consumption reports to the USP implies increased chances of eavesdropping. Such packet leakages may compromise consumer privacy [12] and may be deployed to infer the conditions of home occupancy from captured power consumption reports.

The USP normally analyzes the received consumption reports from the SMs and adjust power transmission appropriately [13]. In so doing, the USP is able to balance peak and off-peak power consumptions [14]. However, attackers may capture and modify the exchanged reports, leading to erroneous adjustments at the USP [2]. As pointed out in [13], demand response management is critical for reliable and efficient power management in SG environment. This requires frequent data exchanges between the SMs and USP. However, this serves to increase chances of the transmitted data being compromised over insecure channels [13]. On the other hand, packet interceptions, modification and eavesdropping have been identified in [15] as being serious threats in SG networks.

The decentralized nature of the SGs, with their massive components and complex connections have been identified in [16] as being the sources of security, trust and privacy issues in this environment. As such, new techniques and protocols are required to deal

with this scenario. Authentication is the first step towards SG network security, which is followed by agreement on some session keys to protect the exchanged packets [4, 17, 18]. The assurance of data privacy, mutual authentication, key establishment, anonymity, untraceability, and unlinkability is critical in SGs. However, the provisioning of these security features at low computation costs is still a challenge [19]. As pointed out in [20], there is need for robust authentication protocols to offer support for secure and private exchange of information among legitimate entities in SGs. The major contributions of this paper include the following:

- Transient security tokens are deployed to dynamically generate the session keys to protect the exchanged power consumption reports.
- All SG network entities communicate using their pseudonyms to uphold their anonymity and untraceability during the authentication and key agreement phase.
- Security analysis is executed to show that the proposed protocol offers superior security features compared with other related schemes.
- Performance evaluation is carried out to show that this protocol provides strong security at the lowest execution times and bandwidth requirements compared with other related protocols.

The rest of this paper is organized as follows: Sect. 2 presents related work while Sect. 3 gives an illustration of the system model adopted in this paper. On the other hand, Sect. 4 presents and discusses the comparative analysis, while Sect. 5 concludes the paper and gives future work.

2 Related Work

Many SG network authentication and key agreement protocols have been presented in literature. For instance, a public and private key based scheme for SMs is presented in [21]. However, this protocol is inefficient due to the intensive computations that must be executed [22, 23]. A SG message authentication technique is introduced in [24], but which is susceptible to DDoS and fails to offer trustworthy mutual authentication [25]. On the other hand, an identity-based encryption protocol is developed in [26]. Although this approach offers mutual authentication and SM anonymity, it cannot assure session key security. In addition, identity-based protocols cannot offer device privacy due to the requirement that the identities be exchanged during mutual authentication [27]. Using elliptic curve cryptography (ECC), a key agreement and authentication (AKA) protocol is presented in [28]. However, this scheme has high communication overheads [7] and is generally complicated.

A blockchain based AKA protocol is introduced in [29] to offer anonymous authentication in SGs. However, the deployed central authority may present some single point of failure [7]. In addition, the blockchain technology employed here has high space and computational complexities [30]. On the other hand, the AKA protocol developed in [31] is still vulnerable to traceability and impersonation attacks. Based on the public key infrastructure (PKI), a lightweight message authentication technique is presented in [32]. However, this protocol has high execution time for the deployed private keys and

signatures [23]. In addition, PKI may lead to unnecessarily heavy storage and signaling complexities among the authenticating entities [33]. Authors in [34] have developed a bilinear maps based protocol, but the deployed bilinear maps render it computationally intensive [30]. In addition, the USP may fail to detect any malicious SM messages [19].

An ECC based lightweight AKA protocol is presented in [35] for clients and SG substations authentication. However, this scheme does not offer perfect key secrecy [36]. To provide protection against outsider and insider attacks in SG, an attribute based security protocol is introduced in [17]. However, the communication and storage costs of this scheme are too high for the computation, transmission and energy limited smart gas meter. On the other hand, the scheme presented in [3] is susceptible to impersonation and ephemeral secret leakage attacks [37]. The PKI based one-way authentication scheme developed in [38] prevented DoS, but has high computation and communication complexities [4]. The SG AKA protocol presented in [39] is unable to offer authentication between two SG entities [40]. On the other hand, the privacy-preserving technique in [41] achieves high privacy but provides only one –way authentication. To secure demand response, an ECC based protocol is developed in [42]. However, this scheme has scalability issues and is devoid of initial verification at the USP side which may lead to malicious requests being processed at the USP.

An identity-based AKA scheme is developed in [23] for SG networks, which was shown to be resilient against impersonation, replay and MitM attacks. However, this protocol is still vulnerable to identity spoofing attacks due to the transmission of SM identity in plain-text [43]. Moreover, the protocols presented in [21, 26, 31, 32] and [44] offer mutual authentication in SG networks at the expense of high computation overheads. On the other hand, authors in [45] have proposed an anonymous authentication protocol for smart grids. However, the scheme in [45] does not consider offline password guessing, privileged insider, physical capture and DoS attacks.

3 System Model

The network entities involved in the proposed protocol include the registration authority (RA), utility service provider (USP), gateway node (GWN) and the smart meter (SM) as shown in Fig. 1.

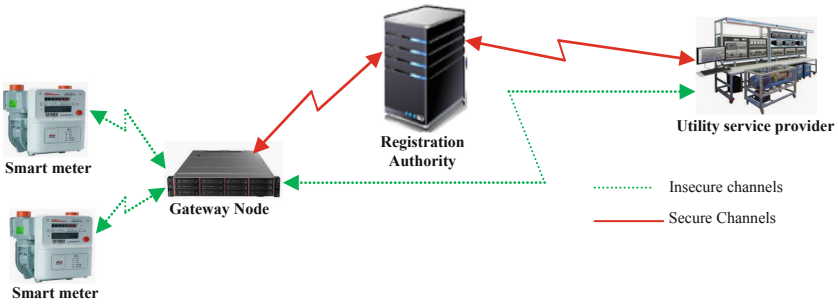

Fig. 1. Network model

As shown in Fig. 1, the smart meters directly communicate with the gateway node, which in turn directly communicated with the registration authority. Similarly, the utility service provider directly communicates with the registration authority. Here, the smart meters measure and submit periodic energy consumption reports to the USP. On the other hand, the USP adjusts power transmission and generation based on the received reports. The registration authority provides the security tokens and parameters needed for the secure transmission and reception of packets over the public channels. As shown in Fig. 1, the communication between the GWN and RA is through secured channels, similar to the connection between RA and USP. However, the communication between SMs and GWN, as well as between USP and GWN is through insecure public channels. Table 1 presents the symbols used in this paper together with their brief descriptions.

Table 1. Symbols

Symbol	Description
RA	Registration authority
USP	Utility service provider
SM	Smart meter
SK_S	SM's secret key
SK_U	USP's secret key
SM_{ID}	SM's identity
PD_{SM}	SM's pseudonym
PID_{USP}	USP's pseudo-identity
PID_S	SM's pseudo-identity
TT_S	SM's transient token
T_{SM}	SM's timestamp during registration
T_{USP}	USP's timestamp during registration
PD_{USP}	USP's pseudonym
ψ $\underline{L}$	USP's login parameters
$\mathbb{H}$	Master symmetric key for RA and GWN
$\underline{T}_i$	Timestamps during AKA
h(.)	One-way hashing operation
$\Delta\underline{T}$	Maximum transmission delays
Å	Session key between SM and USP
$\|\|$	Concatenation operation
$\oplus$	XOR operation

In terms of the execution procedures, the proposed protocol is composed of two major phases, which include registration, followed by authentication and key agreement. The detailed description of these phases is given in the sub-sections below.

3.1 Registration Phase

In this phase, the RA derives master key $\mathbb{H}$, and registers the smart meters and gateway nodes before their actual deployment in the field. To accomplish this, step1 to 5 are utilized.

Step 1: The RA generates shared key SKS and smart meter identity SMID . It then derives the smart meter's pseudonym PDSM = h(SMID||SKS). Next, using prior computed security parameters and the smart meter's current timestamp TSM, the RA derives the smart meter's transient token TTs = h(SMID||SKS||TSM) and additional security parameter $\acute{Z}1$ = h(PDSM||SKS). Afterwards, RA sends {PDS, TTS, $\acute{Z}1$} to the smart meter and gateway node (GWN) through a secure channel.

Step 2: For the utility service provider (USP) to send and receive messages to and from the smart meter, registration at the RA is necessary. This begins by having the USP randomly choose its pseudonym PDUSP and send registration request RegReq together with PDUSP to the RA over some secure channels.

Step 3: Upon receiving Reg_{Req}, RA generates secret key SK_U followed by the derivation of the USP's pseudo-identity PID_{USP} = h(PD_{USP}||SK_U). Next, the RA computes USP's transient token TT_U = h(PD_{USP}||SK_U||T_{USP}). This is followed by the random selection of secret number S that it uses to derive $\mathbb{K}_1$ = h(PD_{USP}||S) and SK_U^* = h(SK_U||$\mathbb{K}_1$). Afterwards, RA sends registration response Reg_{Res} {PID_{USP}, TT_U, $\mathbb{K}_1$, h(.), SK_U^*} to the USP through some secure channels.

Step 4: The SM generates nonce $\eta 3$ and determines current time stamp $\underline{T}5$ that are used to derive the following parameters:

$$\bar{R}=h(\Psi||M),\ P=h(PD_{USP}||\underline{L})\oplus M$$
$$Q=h(PID_{USP}||\bar{R}||\underline{L}||\mathbb{K}_1||TT_U)$$
$$\mathbb{K}_2=\mathbb{K}_1\oplus h(PD_{USP}||M)$$
$$PID_{USP}^*=PID_{USP}\oplus h(M||\Psi)$$
$$TT_U^*=TT_U\oplus h(PD_{USP}||\Psi)$$
$$SK_U^{**}=SK_U^*\oplus h(PD_{USP}||M||\Psi||\underline{L})$$

It then buffers {PID_{USP} *, TT_U *, $\mathbb{K}_2$, P, SK_U **, Q, h(.)} in its memory.

Step 5: Upon successful registration, RA computes $\acute{Z}2$ = h(PIDUSP||SKU), $\acute{Z}3$ = h(PIDS||SKS) and $\acute{Z}4$ = h(SKU||K1) before constructing Msg1 = E$\mathbb{H}$(PDUSP, PIDUSP, TTU, $\acute{Z}2$) and sending it to the GWN. Here, shared key $\mathbb{H}$ is utilized to decrypt Msg1 to yield its contents which are then stored in the GWN's database. As such, this database now contains {PDUSP, PIDUSP, TTU, PIDS, TTS, $\acute{Z}2$, $\acute{Z}3$, $\acute{Z}4$} for subsequent authentication and key agreement. Figure 2 shows the message flows during the registration phase.

As shown in Fig. 2, four messages are exchanged during the registration phase. The RA generates and transmits a number of security parameters to both the USP and GWN. In addition, the GWN and USP perform some decryption and independent derivations of other security tokens to be used for subsequent authentication and key agreement phase.

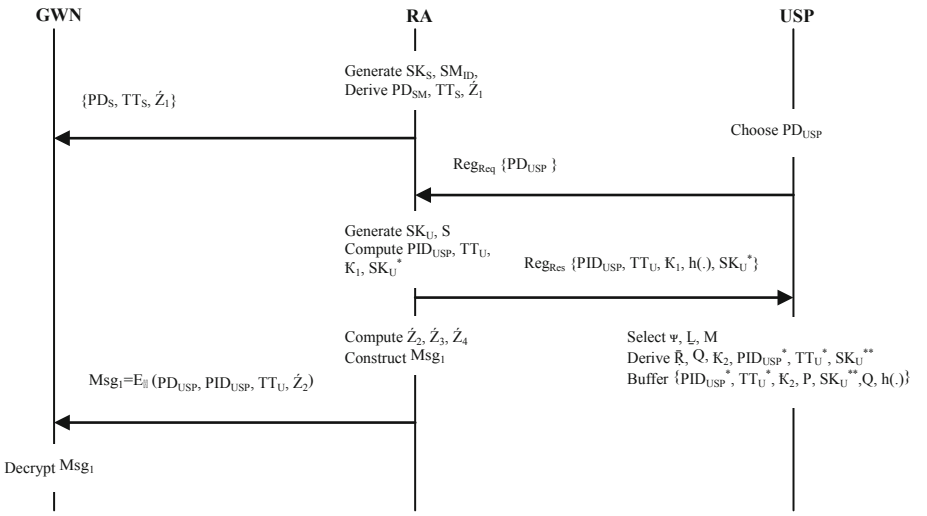

Fig. 2. Registration phase message flows

3.2 Authentication and Key Agreement

This phase is triggered whenever the USP wants to access some data from the remote SM. To accomplish this, the following steps are executed:

Step 1: Using PDUSP, ψ and $\underrightarrow{L}$, the USP derives the following:

$$M=P\oplus h(PD_{USP}||\Psi)$$
$$\bar{K}_1=\bar{K}_2\oplus h(PD_{USP}||M)$$
$$PID_{USP}=PID_{USP}^{*}\oplus h(M||\Psi)$$
$$TT_U=TT_U^{*}\oplus h(PD_{USP}||\underline{L}) \text{ and } \bar{R}=h(\Psi||M)$$
$$Q^{*}=h(PID_{USP}||\bar{R}||\underline{L}||\bar{K}_1||TT_U)$$

It then checks whether Q* = Q and if it is not, authentication is terminated. However, if this check is successful, the USP generates nonce $\eta 1$ and determines the current timestamp $\underline{T}1$. This is followed by the derivation of the following security parameters:

$$SK_U^{**}= SK_U^{*}\oplus h(PD_{USP}||M||\Psi||\underline{L})$$
$$Auth_{M1}=PID_{USP}\oplus h(SK_U^{**}||\underline{T}_1)$$
$$Auth_{M2}=PID_S\oplus h(TT_U||PD_{USP}||\underline{T}_1)$$
$$Auth_{M3}=h(PID_{USP}||TT_U||\underline{T}_1)\oplus \eta_1$$
$$Auth_{M4}=h(PD_{USP}||PID_S||TT_U||\eta_1||\underline{T}_1)$$

Finally, it composes $Msg_2 = \{Auth_{M1}, Auth_{M2}, Auth_{M3}, Auth_{M4}, \underline{T}_1\}$ and sends it to GWN over insecure channels.

Step 2: On receiving Msg_2 from the USP, the GWN determines current timestamp $\underline{T}_2$ before checking whether $|\underline{T}_2 - \underline{T}_1| \leq \Delta\underline{T}$, and if this is not the case, the authentication is terminated. However, if this verification is successful, the GWN derives $PID_{USP} = Auth_{M3} \oplus h(h(SK_U || K_1 || \underline{T}_1)$. Next, it retrieves PD_{USP} and TT_U corresponding to the derived PID_{USP} from its database. This is followed by the derivation of nonce $\eta_1 = Auth_{M3} \oplus h(PID_{USP} || TT_U || \underline{T}_1)$ and $Auth_{M5} = h(PD_{USP} || PID_S || TT_U || \eta_1 || \underline{T}1)$ before verifying that $Auth_{M5} = Auth_{M4}$. If this validation is unsuccessful, the session is terminated, otherwise the GWN generates nonce η_2 and determines the current timestamp $\underline{T}_3$. Next, it derives the following security tokens:

$$Auth_{M6} = h(TT_S || PID_S) \oplus \eta_2$$
$$Auth_{M7} = h(PID_{USP} || TT_U || \eta_1) \oplus h(TT_S || \underline{T}_3)$$
$$Auth_{M8} = h(PID_S || TT_S || h(PID_S || SK_S) || \eta_2 || \underline{T}_3)$$

Finally, it composes Msg3 = {AuthM6, AuthM7, AuthM8,$\underline{T}$3} and transmits it to the SM over insecure channels.

Step 3: Upon receiving Msg3 from GWN, the SM determines current timestamp $\underline{T}4$ and checks whether $|\underline{T}4 - \underline{T}3| \leq \Delta\underline{T}$. If this is not the case, the session is terminated. However, if this condition is true, the SM re-computes the following security tokens:

$$\eta_2 = Auth_{M6} \oplus h(TT_S || PID_S)$$
$$h(PID_{USP} || TT_U || \eta_1) = Auth_{M7} \oplus h(TT_S || \underline{T}_3)$$
$$Auth_{M9} = h(PID_S || TT_S || h(PID_S || SK_S) || \eta_2 || \underline{T}_3)$$

It then confirms whether AuthM9 = AuthM8, and if this condition is false, authentication session is terminated, otherwise the GWN is successfully authenticated by the SM.

Step 4: The SM generates nonce $\eta 3$ and determines current time stamp $\underline{T}5$ that are used to derive the following parameters:

$$Auth_{M10} = h(h(PID_{USP} || TT_U || \eta_1) || \underline{T}_5) \oplus \eta_3$$
$$Auth_{M11} = h(h(PID_{USP} || TT_U || \eta_1) || PID_S || \underline{T}_5) \oplus h(h(PID_S || SK_S) || \underline{T}_5)$$
$$Å = h(h(h(PID_S || SK_S) || \underline{T}_5) || h(PID_{USP} || TT_U || \eta_1) || PID_S || \eta_3 || \underline{T}_5)$$
$$Auth_{M12} = h(Å || \underline{T}_5)$$

Thereafter, it constructs $Msg_4 = \{Auth_{M10}, Auth_{M11}, Auth_{M12}, \underline{T}_5\}$ before transmitting it to the USP through some public channels.

Step 5: Upon receiving Msg_4, the USP determines current timestamp $\underline{T}_6$ and checks whether $|\underline{T}_6 - \underline{T}_5| \leq \Delta\underline{T}$, and if this is false, the session is terminated. However, if this condition is true, the USP derives the following security parameters:

$$\eta_3 = Auth_{M10} \oplus h(h(PID_{USP}||TT_U||\eta_1)||T_5)$$
$$h(h(PID_S||SK_S)||T_5 = Auth_{M11} \oplus h(h(PID_{USP}||TT_U||\eta_1)||PID_S||T_5)$$
$$Å^* = h(h(h(PID_S||SK_S)||T_5)||h(PID_{USP}||TT_U||\eta_1)||PID_S||\eta_3||T_5)$$
$$Auth_{M13} = h(Å^*||T_5)$$

This is followed by the confirmation of whether $Auth_{M13} = Auth_{M12}$ and if this is not the case, the authentication is terminated, otherwise the SM is authenticated by the USP. As such, the computed session key $Å^*$ derived at the USP is valid and both the USP and SM set $Å^* = Å$ as the shared session key to protect the exchanged packets. Figure 3 shows the message flows during the authentication and key agreement phase.

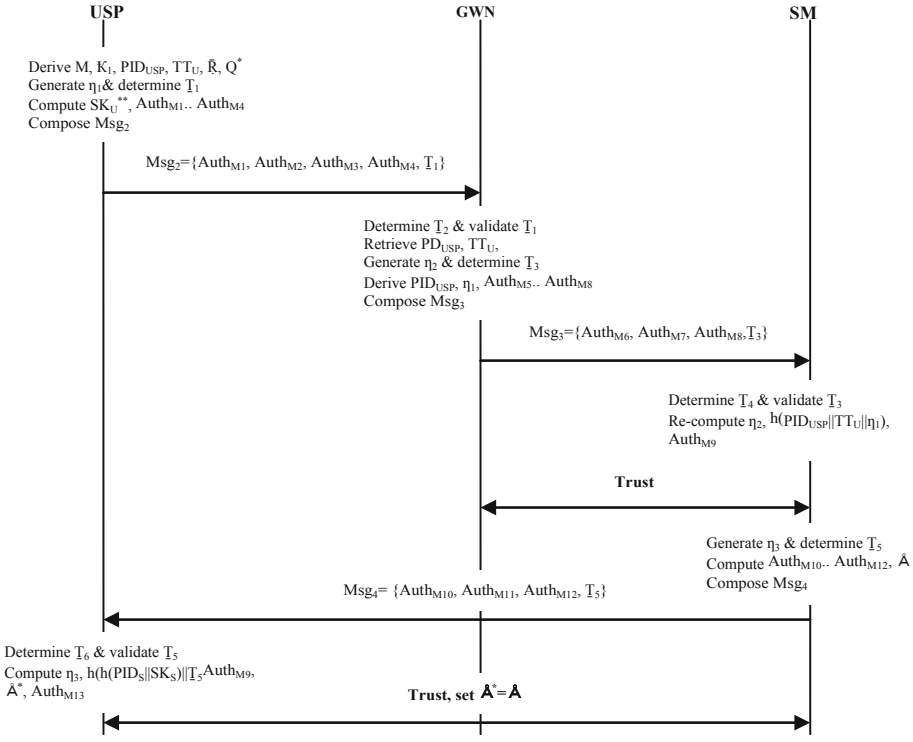

Fig. 3. Authentication and key agreement phase

Based on Fig. 3, a total of three messages are exchanged during the authentication and key agreement phase. It is also evident that each of the network entity independently computes a number of ephemeral security parameters that are then deployed to verify the received messages before some trust levels can be established among all the communicating entities.

4 Results and Discussion

In this section, the security and privacy features provided by the proposed protocol are analyzed as elaborated in Sect. 4.1. In addition, the performance evaluation in terms of execution time and bandwidth requirements is provided in Sect. 4.2 below.

4.1 Security Evaluation

To show the robustness of the proposed protocol against some of the typical smart grid attacks, the following eight

Theorem 1: DoS Attacks are Sufficiently Prevented in the Proposed Protocol.

Proof: During the authentication and key agreement procedures, the USP security parameters PD_{USP}, ψ and $\underset{\rightarrow}{L}$ are verified through the confirmation of whether $Q^* = Q$. As such, the authentication request message $Msg_2 = \{Auth_{M1}, Auth_{M2}, Auth_{M3}, Auth_{M4}\}$ is transmitted towards the GWN upon successful local authentication. Devoid of this successful local verification, authentication request cannot be sent over to the GWN. The incorporation of timestamps and random nonces renders the computed authentication parameters stochastic and hence cannot be easily determined by an adversary for possible session hijacking and hence DoS for the legitimate entities.

Theorem 2: Anonymity and Untraceability are Upheld in the Proposed Protocol.

Proof: In the proposed protocol, timestamps $\underset{\sim}{T}_1$, $\underset{\sim}{T}_2$, $\underset{\sim}{T}_3$, $\underset{\sim}{T}_4$, $\underset{\sim}{T}_5$ and $\underset{\sim}{T}_6$ are deployed in all exchanged messages Msg_2, Msg_3 and Msg_4. The same also applies to random nonces η_1, η_2 and η_3 during the authentication and key agreement. Consequently, all the exchanged messages are session specific and hence an adversary is unable to trace the GWN or the SM during the communication process. In addition, pseudo-identities PID_{USP} and PID_S are components of the exchanged messages Msg_2, Msg_3 and Msg_4. Since both PID_{USP} and PID_S are protected by a one-way hashing operation, they cannot be reversed to decipher their contents. This is due to the collision-resistance feature of the one-way hashing operation.

Theorem 3: The Proposed Protocol is Resilient Against Replay Attacks.

Proof: In the proposed protocol, timestamps are incorporated in the exchanged messages Msg_2, Msg_3 and Msg_4 during authentication and key agreement procedures. Upon receipt of each of these messages, freshness checks are executed using the timestamps in these messages as well as the permissible transmission delay $\Delta\underset{\sim}{T}$. Consequently, an attacker is unable to intercept, modify and forward the transmitted messages due to the little transmission delays permitted.

Theorem 4: The Proposed Protocol Preserves Forward Key Secrecy.

Proof: Suppose that an adversary has intercepted exchanged messages Msg_2, Msg_3 and Msg_4 during the authentication and key agreement phase. Since $Å = h(h(h(PID_S||SK_S)||T_5)||h(PID_{USP}||TT_U||\eta_1)||PID_S||\eta_3||T_5)$, the security of the session key is dependent on long term keys PID_{USP}, PID_S, TT_U, SK_S and ephemerals η_1 and η_3. If an attacker eavesdrops timestamps T_1 and T_5, followed by secrets η_1 and η_3, still the session key Å cannot be derived. This is because it requires long terms secrets PID_{USP}, PID_S, TT_U and SK_S. Conversely, without knowledge of short term secrets η_1 and η_3, the session key Å cannot be computed. As such, an adversary can only derive Å when both short term and long terms secrets are known, which is cumbersome.

Theorem 5: Man-in-the-Middle Attacks Are Thwarted in the Proposed Protocol.

Proof: In this attack, it is assumed that an attacker has eavesdropped $Msg_2 = \{Auth_{M1}, Auth_{M2}, Auth_{M3}, Auth_{M4}, T_1\}$. Thereafter, an attempt is made to alter this message and replay it later on. Here:

$$Auth_{M1}=PID_{USP}\oplus h(SK_U^{**}||T_1)$$
$$Auth_{M2}=PID_S\oplus h(TT_U||PD_{USP}||T_1)$$
$$Auth_{M3}=h(PID_{USP}||TT_U||T_1)\oplus \eta_1$$
$$Auth_{M4}=h(PD_{USP}||PID_S||TT_U||\eta_1||T_1)$$

To carry out this modification, an adversary generates nonce η_1^* and timestamp T_1^*, then computes $Auth_{M1}^* = PID_{USP} \oplus h(SK_U^{**}||T_1^*)$ to substitute in Msg_2. However, devoid of long terms secrets PID_{USP}, PD_{USP}, and SK_U^{**}, the attacker is unable to derive valid message Msg_2 nor can other messages exchanged during the authentication and key agreement process be derived.

Theorem 6: The Proposed Protocol is Resilient Against Impersonation Attacks.

Proof: Suppose that an attacker masquerading as USP attempts to establish an authentication session with the GWN. To construct a valid authentication message $Msg_2^* = \{Auth_{M1}^*, Auth_{M2}^*, Auth_{M3}^*, Auth_{M4}^*, T_1^*\}$ for this impersonation, the adversary needs to generate current timestamp T_1^A and nonce η_A. However, without valid security parameters PID_{USP}, PID_S and SK_U, it is infeasible to compute TT_U, $Auth_{M1}^*$, $Auth_{M2}^*$, $Auth_{M3}^*$ and $Auth_{M4}^*$. As such, an attacker is unable to generate valid Msg_2^* and hence this attack flops.

Let us assume that the adversary is interested in masquerading as GWN by generating current timestamp T_3^*, nonces η_1^* and η_2^*. Thereafter, an attempt is made to transmit message $Msg_3^* = \{Auth_{M6}, Auth_{M7}, Auth_{M8}, T_3^*\}$ to the SM. However, devoid of valid PID_{USP}, PID_S and SK_S, it is impossible to derive $Auth_{M6}^*$, $Auth_{M7}^*$ and $Auth_{M8}^*$ and hence is unable to generate valid Msg_3^*. Suppose that an attacker generates timestamp T_5^*, and nonces η_1^* and η_3^*. Thereafter, an attempt is made to construct and send bogus message $Msg_4^* = \{Auth_{M10}^*, Auth_{M11}^*, Auth_{M12}^*, T_5^*\}$ to the USP. However, without valid PID_{USP}, PID_S and SK_S, it is impossible to derive $Auth_{M10}^*$, $Auth_{M11}^*$ and $Auth_{M12}^*$, and hence this attack fails.

Theorem 7: The Proposed Protocol is Robust Against Physical Capture Attacks.

Proof: The assumption made here is that an adversary has captured the smart meter and has obtained secrets $\{PD_S, TT_S, h(PD_S||SK_S)$ from the SM's memory. However, in the proposed protocol, security parameters $\{PD_S, TT_S, h(PD_S||SK_S)$ are assigned by the RA and hence are quite distinct for each SM in the smart grid network. As such, the physical capture of one SM only yields the session key deployed between the SM and the USP. Consequently, the session keys established between other SMs and the USP cannot be obtained by the attacker, and hence their security is still intact.

Theorem 8: Offline Password Guessing and Privileged Insider Attacks are Thwarted in the Proposed Protocol.

Proof: Suppose that some privileged insider intercepts $\{PD_{USP}\}$ sent from the USP towards the RA during the registration phase. It is also assumed that this privileged insider has utilized power analysis to retrieve security set $\{PID_{USP}^*, TT_U^*, \mathbb{K}_2, P, SK_U^{**}, Q, h(.)\}$ from memory. Thereafter, an attempt is made to derive $M = P \oplus h(PD_{USP}||\psi)$. However, without knowledge of security token ψ, this computation fails since it cannot be determined from the captured memory parameters. Similarly, without M, security parameters PD_S and $\bar{R} = h(\psi||M)$ cannot be computed. Table 2 presents the security robustness comparisons of the proposed protocol with other related schemes.

Table 2 Attack model comparisons

Attack model	[23]	[35]	[4]	[45]	Proposed
Offline password guessing	–	–	–	–	√
Privileged insider	–	–	–	–	√
Physical capture	–	–	–	–	√
Impersonation	√	√	√	√	√
MitM	√	√	√	√	√
Forward key secrecy	√	√	√	√	√
Replay	√	√	√	√	√
Anonymity	x	x	√	√	√
Untraceability	x	x	–	√	√
DoS	–	–	–	–	√
Mutual authentication	√	√	√	√	√

Legend
√ Effective
x Ineffective
– Not considered

It is evident from Table 2 that the proposed protocol offers the highest number of security features compared with the other related schemes.

4.2 Performance Analysis

In this sub-section, the proposed protocol is evaluated in terms of the number of bytes exchanged during the authentication and key agreement phase. In addition, the execution time for the various cryptographic operations is also provided as discussed below.

Bandwidth Requirements: During the authentication and key agreement phase, messages $Msg_2 = \{Auth_{M1}, Auth_{M2}, Auth_{M3}, Auth_{M4}, \underline{T}_1\}$, $Msg_3 = \{Auth_{M6}, Auth_{M7}, Auth_{M8}, \underline{T}_3\}$ and $Msg_4 = \{Auth_{M10}, Auth_{M11}, Auth_{M12}, \underline{T}_5\}$ are exchanged. Using the values in [45] and [46], the outputs of the various cryptographic operations are given in Table 3 below.

Table 3. Cryptographic output sizes

Operation	Output size (bytes)
EC point addition	40
EC point multiplication	40
HMAC	20
SHA 1	16
AES-128 encryption	16
AES-128 decryption	16
Identity	20
Timestamp	4
Random nonce	16

As shown in Table 3, elliptic curve (EC) point encryption and decryption outputs are 40 bytes long while the Hash-based Message Authentication Code (HMAC) output is 20 bytes. On the other hand, random nonce, one-way hashing, advanced encryption standard (AES) encryption and decryption are 16 bytes each. In addition, timestamp and device identity are 4 bytes and 20 bytes long respectively. Based on these values, the bandwidth requirement of the proposed protocol is computed as follows:

$Msg_2 = \{Auth_{M1} = Auth_{M2} = Auth_{M3} = Auth_{M4} = 16, \underline{T}_1 = 4\} = 68$ bytes.
$Msg_3 = \{Auth_{M6} = Auth_{M7} = Auth_{M8} = 16, \underline{T}_3 = 4\} = 52$ bytes.
$Msg_4 = \{Auth_{M10} = Auth_{M1} = Auth_{M12} = 16, \underline{T}_5 = 4\} = 52$ bytes

Consequently, the total bandwidth requirement in the proposed protocol is 172 bytes. On the other hand, the schemes in [4, 23, 35, 45] have bandwidth requirements of 248 bytes, 298 bytes, 254 bytes and 204 bytes respectively, as shown in Fig. 4.

It is evident from Fig. 4 that the authentication protocol in [35] has the highest bandwidth requirements while the proposed protocol has the least bandwidth requirements. As such, this protocol is the most applicable in a smart grid environment where most devices are energy constrained.

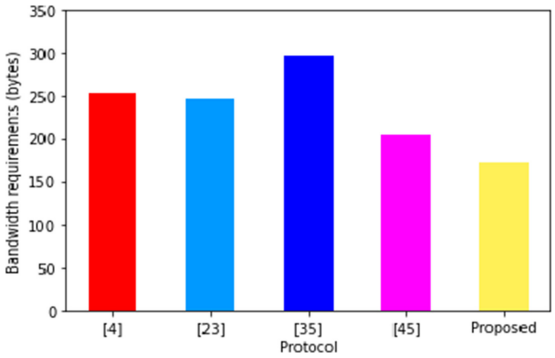

Fig. 4. Bandwidth requirements comparisons

Table 4. Execution times comparisons

Scheme	Execution time (ms)
[45]	0.347
[4]	17.306
[35]	15.965
[23]	15.693
Proposed	0.05678

Execution Time: In a typical authentication scheme, one-way hashing T_H, symmetric encryption T_E, symmetric decryption T_D, elliptic curve point multiplication T_{EM}, elliptic curve point addition T_{EA} and Hash-based Message Authentication Code T_{HMAC} are some of the cryptographic operations carried out. In the proposed protocol, 17 one-way hashing operations are executed on the USP side while 8 hashing operations are executed on the gateway node. On the other hand, 9 hashing operations are carried out on the smart meter side. As such, the total computation overhead is 34 hashing operations. Using the values in [45], T_H, T_E, T_D and T_{EM} operations consume 0.00167 ms, 0.0225 ms, 0.042 ms and 7.5045 ms respectively. As such, the total execution time in the proposed protocol is 0.05678 ms as shown in Table 4.

The scheme in [23] requires $7T_H$ and $5T_{EM}$ operations while the protocol in [35] needs $5T_H$, $5T_{EM}$ and $1T_{EA}$ operations. On the other hand, the scheme in [4] requires $7T_H$, $2T_E$, $2T_D$, $5T_{EM}$ and $4T_{HMAC}$ operations, while the protocol in [45] needs $16T_H$, $2T_D$ and $2T_E$ operations. This explains their high executions times compared with the proposed protocol. Since the proposed protocol has the least execution times, it does not overwhelm the processors and hence is the most ideal for SG devices that are characterized by limited computational power.

5 Conclusion and Future Work

Majority of the conventional smart grid security schemes have been noted to be based on public key infrastructure, blockchain, elliptic curve cryptography and bilinear pairing operations. However, inefficiency and susceptibility to numerous attacks are some of the shortcomings of these security solutions. Owing to the criticality of strong authentication, information privacy, key establishment, untraceability, anonymity and unlinkability, a novel security protocol is presented in this paper. It is shown that this protocol offers these security features at the least execution times and bandwidth requirements. In addition, it is demonstrated to be resilient against smart grid attack vectors such as offline password guessing, denial of service, packet replays, privileged insider, man-in-the-middle, impersonation and physical capture. Consequently, this protocol is ideal for deployment in smart gas meters as well as in other smart grid devices with limited computation, transmission and energy. Future work in this domain lies in the formal verification of the security features provided by this protocol.

References

1. Mollah, M.B., et al.: Blockchain for future smart grid: A comprehensive survey. IEEE Internet Things J. **8**(1), 18–43 (2020)
2. Nyangaresi, V.O., Mohammad, Z.: Privacy preservation protocol for smart grid networks. In: 2021 International Telecommunications Conference (ITC-Egypt), pp. 1–4, IEEE (2021)
3. Mahmood, K., et al.: Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure. Futur. Gener. Comput. Syst. **88**, 491–500 (2018)
4. 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**, 4349–4359 (2018)
5. Nyangaresi, V.O., Alsamhi, S.H.: Towards secure traffic signaling in smart grids. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 196–201 (2021)
6. Sureshkumar, V., Anandhi, S., Amin, R., Selvarajan, N., Madhumathi, R.: Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication. IEEE Syst. J. **15**(3), 3565–3572 (2020)
7. Wang, W., Huang, H., Zhang, L., Su, C.: Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Netw. Appl. **14**(5), 2681–2693 (2020). https://doi.org/10.1007/s12083-020-01020-2
8. Saxena, N., Choi, B.J.: Integrated distributed authentication protocol for smart grid communications. IEEE Syst. J. **12**(3), 2545–2556 (2018)
9. Nyangaresi, V.O. Ogundoyin, S.O.: Certificate based authentication scheme for smart homes. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 202–207 (2021)
10. Nyangaresi, V.O.: ECC based authentication scheme for smart homes. In: 2021 International Symposium ELMAR, pp. 5–10. IEEE (2021)
11. Liu, S., et al.: Model-free data authentication for cyber security in power systems. IEEE Trans. Smart Grid **11**(5), 4565–4568 (2020)
12. 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)

13. Chaudhry, S.A., Alhakami, H., Baz, A., Al-Turjman, F.: Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure. IEEE Access **8**, 101235–101243 (2020)
14. Guan, Z., Zhang, Y., Zhu, L., Wu, L., Yu, S.: Effect: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. Sci. China Inf. Sci. **62**(3), 32103 (2019)
15. Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., Kim, S.W.: Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. IEEE Access **8**, 24746–24772 (2020)
16. Ghosal, A., Conti, M.: Key management systems for smart grid advanced metering infrastructure: a survey. IEEE Commun. Surv. Tutor. **21**(3), 2831–2848 (2019)
17. Saxena, N., Choi, B.J., Lu, R.: Authentication and authorization scheme for various user roles and devices in smart grid. IEEE Trans. Inf. Forensics Secur. **11**(5), 907–921 (2016)
18. Nyangaresi, V.O.: Lightweight key agreement and authentication protocol for smart homes. In: 2021 IEEE AFRICON, pp. IEEE (2021)
19. Braeken, A., Kumar, P., Martin, A.: Efficient and provably secure key agreement for modern smart metering communications. Energies **11**(10), 26–62 (2018)
20. Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S.A., Rahman, A.U., Najmus Saqib, M.: Security and key management in IoT-based wireless sensor networks: an authentication protocol using symmetric key. Int. J. Commun. Syst. **32**(16), e4139 (2019)
21. Nicanfar, H., Jokar, P., Beznosov, K., Leung, V.: Efficient authentication and key management mechanisms for smart grid communications. IEEE Syst. J. **8**(2), 629–640 (2014)
22. Saxena, N., Choi, B.J.: State of the art authentication, access control, and secure integration in smart grid. Energies **8**(10), 11883–11915 (2015)
23. 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)
24. Li, X., Wu, F., Kumari, S., Xu, L., Sangaiah, A.K., Choo, K.K.R.: A provably secure and anonymous message authentication scheme for smart grids. J. Parallel. Distrib. Comput. **132**, 242–249 (2019)
25. Wu, L., Wang, J., Zeadally, S., He, D.: Anonymous and efficient message authentication scheme for smart grid. Secur. Commun. Netw. **2019**, 1–13 (2019)
26. Tsai, J., Lo, N.: Secure anonymous key distribution scheme for smart grid. IEEE Trans. Smart Grid **7**(2), 906–914 (2016)
27. 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
28. Garg, S., Kaur, K., Kaddoum, G., Rodrigues, J.J.P.C., Guizani, M.: Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. IEEE Trans. Industr. Inf. **16**(5), 3548–3557 (2019)
29. 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. Industr. Inf. **16**(3), 1984–1992 (2019)
30. 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)
31. Odelu, V., Kumar Das, A., Wazid, M., Conti, M.: Provably secure authenticated key agreement scheme for smart grid. IEEE Trans. Smart Grid **9**(3), 1900–1910 (2018)

32. Mahmood, K., Chaudhry, S.A., Naqvi, H., Shon, T., Ahmad, H.F.: A lightweight message authentication scheme for smart grid communications in power sector. Comput. Electr. Eng. **52**, 114–124 (2016)
33. Nyangaresi, V.O.: Hardware assisted protocol for attacks prevention in ad hoc networks. In: Miraz, M.H., Southall, G., Ali, M., Ware, A., Soomro, S. (eds.) iCETiC 2021. LNICSSITE, vol. 395, pp. 3–20. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90016-8_1
34. 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)
35. 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. Futur. Gener. Comput. Syst. **81**, 557–565 (2018)
36. Abbasinezhad-Mood, D., Nikooghadam, M.: Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. Futur. Gener. Comput. Syst. **84**, 47–57 (2018)
37. Liang, X.-C., Wu, T.-Y., Lee, Y.-Q., Chen, C.-M., Yeh, J.-H.: Cryptanalysis of a pairing-based anonymous key agreement scheme for smart grid. In: Pan, J.-S., Li, J., Tsai, P.-W., Jain, L.C. (eds.) Advances in Intelligent Information Hiding and Multimedia Signal Processing. SIST, vol. 156, pp. 125–131. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-9714-1_14
38. He, D., Chan, S.C., Zhang, Y., Guizani, M., Chen, C., Bu, J.: An enhanced public key infrastructure to secure smart grid wireless communication networks. Netw. IEEE **28**(1), 10–16 (2014)
39. Challa, S., et al.: Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems. Futur. Gener. Comput. Syst. **108**, 1267–1286 (2018)
40. Chaudhry, S.A., Shon, T., Al-Turjman, F., Alsharif, M.H.: Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems. Comput. Commun. **153**, 527–537 (2020)
41. Chim, T.W., Yiu, S.M., Li, V.K., Hui, L.K., Zhong, J.: PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. IEEE Trans. Dependable Secure Comput. **12**(1), 85–97 (2015)
42. Kumar, N., Aujla, G.S., Das, A.K., Conti, M.: Eccauth: a secure authentication protocol for demand response management in a smart grid system. In: IEEE Trans. Ind. Inform.**15**, 6572–6582 (2019)
43. Mahmood, K., Arshad, J., Chaudhry, S.A., Kumari, S.: An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure. Int. J. Commun. Syst. **32**(16), e4137 (2019)
44. 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)
45. Zhang, L., Zhao, L., Yin, S., Chi, C.H., Liu, R., Zhang, Y.: A lightweight authentication scheme with privacy protection for smart grid communications. Futur. Gener. Comput. Syst. **100**, 770–778 (2019)
46. Wazid, M., Das, A.K., Bhat, V., Vasilakos, A.V.: LAM-CIoT: lightweight authentication mechanism in cloud-based IoT environment. J. Netw. Comput. Appl. **150**, 102496 (2020)