The ISC Int'l Journal of Information Security

July 2024, Volume 16, Number 2 (pp. 1–12)

http://www.isecure-journal.org

An Authenticated Key Establishment Protocol with Perfect Forward Secrecy in Smart Grids

Mustafa Husam Shareef Alrzij [1] and Maryam Rajabzadeh Asaar [1,*]

[1] *Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Sattari St., 10587, Tehran, Iran*

ARTICLE INFO.

Article history:
Received:
Revised:
Accepted:
Published Online:

Keywords:
Key Establishment, Mutual Authentication, Smart Grid

Type: Research Article

doi:

dor:

ABSTRACT

In smart grids, messages exchanged between service providers and smart meters should be authenticated and confidential to prevent threats due to their insecurity. Hence, it is imperative to design a secure authentication and key exchange scheme to create a session key for secure and authenticated transmission of messages. In this paper, we show that the mutual authentication and key establishment protocol presented by Sureshkumar *et al.* in 2020, which is based on the elliptic curve cryptography (ECC), fails to satisfy forward secrecy, while they claimed that it provides perfect forward secrecy. In addition, it will be demonstrated that it is not secure against stolen database attacks of a service provider, which leads to the smart meter impersonation and session key exposure attacks. Moreover, we prove that it fails to achieve security against known session-specific temporary information attacks. Next, an improved authenticated key establishment protocol to address these vulnerabilities has been proposed. Then, we analyze its security with informal and formal methods, such as Burrow-Abadi-Needham (BAN) logic and ProVerif. Finally, comparing security features and computation and communication overhead shows that it outperforms baseline papers.

1 Introduction

A smart grid is a network that manages electric power production and distribution in a reliable, efficient and sustainable method [1, 2], and based on the user demand, it is possible to adjust their consumption. Smart meters, service providers and control centers are principal components in a typical smart grid, where smart meters are equipment for monitoring the power stability of the network and power consumption at arranged periods [3, 4]. Service providers dedicate power resources to the users with the help of gathered data from smart meters [5]. Data transmission in the insecure smart grid network is an imperative challenge, and some of the most critical security requirements are given in what follows [6–8].

- Security against different attacks: The scheme should resist impersonation attacks, stolen service provider database attacks and known session-specific temporary information attacks.
- Perfect forward secrecy: The scheme should provide forward secrecy, which means if long-term secret keys of entities are compromised, session keys cannot be extracted.
- Anonymity, untraceability and unlinkability: The scheme should guarantee these features for

* Corresponding author.
Email addresses: mustafahusam007@gmail.com, m.r.asaar@iau.ac.ir

ISSN: 2008-2045

SMs, where no one from a message finds its origin, nobody can find the sender of a message, and no one can link two messages.

Lots of authentication protocols with session key distribution properties have been proposed to achieve these security requirements. In 2020, Sureshkumar *et al.* [9] gave an ECC-based authenticated key establishment protocol to create a session key between the service provider and the smart meter to provide secure data transmissions, while it will be shown that it is not secure by presenting some vulnerabilities. Xia *et al.* [10], in 2023, gave a provably secure authenticated key exchange protocol to provide mutual authentication and explicit session key confirmation. However, it is vulnerable to known session-specific temporary information attacks because the session key is calculated if ephemeral random numbers are exposed. Furthermore, their scheme is not practical and efficient because it employs zero-knowledge proofs.

Currently, Chai *et al.* [11] proposed an efficient ECC-based authentication protocol suitable for devices with limited resources. At the same time, their scheme does not support perfect forward secrecy since session keys are obtained with revealing long-term secret keys. Furthermore, it is vulnerable to the known session-specific temporary information attacks since the long-term keys, and consequently, session keys are obtained in case of exposing ephemeral random numbers. Moreover, it cannot guarantee the anonymity of smart meters because the real identities of smart meters are extracted from the parameters on the public channels. In addition, Egide and Li [12] presented another ECC-based authentication protocol for smart grids, in which entities with different cryptographic systems can communicate to generate a secure session key. Unfortunately, their scheme suffers from known session-specific temporary information attacks, and the anonymity of smart meters is not preserved. Moreover, it cannot provide perfect forward secrecy.

In 2023, Badar *et al.* [13] presented an efficient ECC-based mutual authentication scheme to provide surveillance to smart meters in smart grid infrastructure, they showed that it is secure in the random oracle model. However, some of them cannot provide untraceability and unlinkability properties [4, 12, 14, 15], others fail to achieve perfect forward secrecy, security against known session-specific temporary information and smart meter impersonation attacks [10, 12]. Therefore, most of the recent schemes are either insecure [9–12] or inefficient in computation and communication overheads [10] to be used in smart grids. Consequently, presenting an authenticated key establishment scheme, which supports all security features, especially perfect forward secrecy and has reasonable performance, is challenging [4, 9, 11, 13, 14, 16].

1.1 Our Contribution

The significant contributions of this paper are listed as follows.

- We analyze the authentication protocol presented by Sureshkumar *et al.* [9] in 2020 and show that it is not forward secure and also not secure against stolen database attacks of a service provider. Consequently, it is vulnerable to smart meter impersonation attacks. Furthermore, it fails to achieve security against known-session-specific temporary information attacks. Then, a modified authentication protocol is proposed, which tackles the weaknesses above.
- In the formal security analyses, it is shown that it accomplishes session key security by using BAN logic and ProVerif. In addition, we informally prove that our protocol is secure against various known attacks, such as smart meter impersonation attacks, and it also satisfies forward secrecy.
- Finally, the evaluation of our protocol in terms of security properties and communication and computation overheads is given, and we compare the results with related schemes to show that it can achieve the security requirements of smart grids and has reasonable communication and computation costs.

1.2 Related Work

A smart grid is an infrastructure that produces and distributes electricity through smart communication. Various studies have been done to guarantee security and privacy in the communication. Wu and Zhou in 2011 [17] gave an elliptic curve cryptography (ECC)-based key distribution protocol which employs symmetric key protocol presented by Needham Schroeder, and they showed that their scheme is resistant against man-in-the-middle attacks. Unfortunately, in 2012 Xia and Wang [18] indicated that the protocol given by Wu and Zhou [17] suffers from man-in-the-middle attacks, and they presented a lightweight directory access protocol (LDAP)-based key distribution scheme. Park and Kim [19] showed that the protocol presented by Xia and Wang [18] fails to have security against impersonation attacks and also suffers from single-point failure. In addition, it cannot support smart meter privacy, and it is not practical due to the online involvement of TA in every communication between a service provider and a smart meter. Liu *et al.* [20] in 2013 presented a key management scheme with lower computational cost for smart meters, while Wang *et al.* [21] in 2014 showed that the scheme presented by

Liu *et al.* [20] is not secure against de-synchronization attacks, also gave a key management scheme using bilinear pairings to address these vulnerabilities. However, the computational cost is increased due to the use of bilinear pairings. In 2016, Tsai and Lo [22] proposed a mutual authentication scheme based on identity-based cryptography to provide smart meter privacy and efficiency. In 2016, Odelu *et al.* [23] proved that the protocol presented by Tsai and Lo [22] does not satisfy the privacy of smart meter credentials and also session key security in Canetti-Krawczyk (CK) model [24, 25], and gave a modified scheme to be secure against these vulnerabilities. Next, Chen *et al.* [3] demonstrated that their scheme fails to have security against impersonation attacks and untraceability. Then, they presented an authentication protocol based on bilinear pairings that is secure under the Diffie-Hellman problem in the random oracle model and the BAN logic, while it has lower performance.

In 2020, Sureshkumar *et al.* [9] gave an ECC-based authentication protocol which employs a key establishment protocol to generate a session key between the service provider and the smart meter. Then, it is shown that the proposed protocol is sound using informal and formal analysis. In 2023, Xia *et al.* [10] proposed a provably secure authenticated key exchange protocol using tightly secure digital signatures over finite fields to satisfy explicit session key confirmation and mutual authentication. However, it is not resistant to known session-specific temporary information attacks since the session key is compromised if ephemeral random numbers are leaked. In addition, their proposal is not lightweight since it employs zero-knowledge proofs.

Similarly, Chai *et al.* [11] presented a secure and lightweight ECC-based authentication protocol which supports devices with limited computing capabilities. However, their scheme does not support perfect forward secrecy since session keys are obtained in case of revealing long-term secret keys. Furthermore, it is not resistant to the known session-specific temporary information attacks since the long-term keys and, consequently, session keys are extracted if ephemeral random numbers are exposed. Moreover, it cannot guarantee the anonymity of smart meters because the real identities of smart meters are revealed from the public parameters. Egide and Li [12] gave another ECC-based authentication protocol for smart grids, in which entities with different cryptographic systems can communicate to generate a secure session key. Unfortunately, their scheme is vulnerable to the known session-specific temporary information attacks in which the session key is compromised easily, and the anonymity of smart meters is not preserved. In addition, it cannot provide perfect forward secrecy.

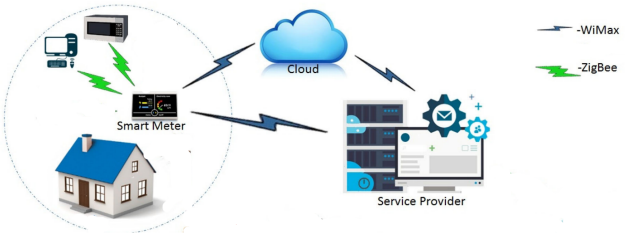

Figure 1. Structure of a smart grid network

Badar *et al.* [13] presented an ECC-based lightweight mutual authentication scheme to offer surveillance to smart meters in smart grid infrastructure, and they showed that it is secure in the random oracle model.

1.3 Organization of the Paper

The rest of this paper is organized as follows. Section 2 presents background information, including the system and security model used in the paper. Section 3 and Section 4 present a review of the Sureshkumar *et al.* scheme and its security vulnerabilities, respectively. Then, the heart of our paper, our improved scheme and its security analysis, are presented in Section 5 and Section 6. This is the main contribution of our work, offering a novel and robust security solution. Section 7 and Section 8 present evaluation and conclusion, respectively.

2 Preliminaries

2.1 System Model

Our system model is based on the system model presented by Sureshkumar *et al.* [9] that is reviewed here. Smart meters (SMs) are connected to smart homes, which consist of smart devices such as tablets. Service providers (SPs) are smart grid entities where SMs regularly transfer data related to energy consumption to cloud servers. The SPs can access the data uploaded into the cloud and monitor power consumption, as shown in Figure 1 [9]. Hence, there is a connection between SMs and SPs because energy consumption data are regularly updated by SMs and can be used by SPs, where this transmission may be insecure due to the insecure nature of smart grids. As a consequence, there is a need to make the data transfer secure using a secure and efficient authenticated key establishment protocol.

2.2 Adversary Model

In this subsection, the capabilities of adversaries based on the Dolev-Yao (DY) model [26] in smart grid environments are listed in what follows [27–29]

- The adversary can eavesdrop, modify, and insert

transmitted messages between SPs and SMs in the smart grid network.
- The adversary knows previous session keys created between SPs and SMs.
- The adversary knows ephemeral secret values of SMs in a session.
- The adversary can know the long-term secret key of SP.
- The adversary can have access to the database of SP and can extract its stored information.
- The adversary can be registered as a legal smart meter in the smart grids and gets all related secret information.

2.3 Security Requirements

A mutual authenticated key establishment protocol should provide the following security requirements [2, 3, 7, 9, 14, 22, 23, 30].

- **Data privacy.** Transmitted messages in the network should be confidential so that an adversary can't eavesdrop on them and take advantage of them [2].
- **Mutual authentication.** Both parties, service providers and smart meters should be authenticated by each other to prevent man-in-the-middle attacks and impersonation attacks [14].
- **Key establishment.** A session key has to be generated between a service provider and a smart meter after mutual authentication to be used for confidentiality, integrity and authentication of messages exchanged through the network [16, 23].
- **Anonymity.** The real identity of smart meters should be hidden from anyone who monitors the network to avoid adversarial control on smart meters [22, 30].
- **Perfect forward secrecy.** The previous session keys should not be compromised if long-term secret keys of smart meters and service providers are leaked [9].
- **Untraceability.** Transmitted messages from one smart meter should not be related to that smart meter, and an adversary cannot find which message is sent by the smart meter [22, 23].
- **Unlinkability.** Transmitted messages from one smart meter should not be linked to each other, and an adversary cannot distinguish which messages have been sent by one smart meter [2, 3].
- **Security against the stolen database of service providers.** Smart meter impersonation attacks cannot be done, or session keys cannot be obtained if stored information in the service provider's database is leaked.
- **Security against known session-specific temporary information attacks.** The session keys cannot be extracted if ephemeral secret values are leaked.

3 Review of Sureshkumar *et al.*'s Scheme

In this section, the details of the protocol presented by Sureshkumar *et al.* [9] are reviewed in order to present its security drawbacks in the next section. First of all, the notations used throughout the paper will be introduced.

Table 1. Notations

Notation	Description
id_i	Identity of smart meter SM_i
P	The generator of group G
x_i	Secret key of SM_i
x_{sp}	Secret key of SP
P_i	Public key of SM_i
P_{sp}	Public key of SP
RTS_i	a random temporary string
K_i	Secret key of SP for the smart meter SM_i
PID_i	Pseudo identity of SM_i
a, w	Random numbers selected by the smart meter
r	Random number selected by SP
T_j	Time stamp for $j = 1$ to $j = 4$
SK	Session key between SP and SM
$E_{x_{sp}}(.)/D_{x_{sp}}(.)$	Symmetric encryption/ decryption by x_{sp}
$h(.)$	One-way hash function
$\oplus$	XOR operation

3.1 Setup

The service provider SP selects an elliptic curve $E(\alpha, \beta) : y^2 = x^3 + \alpha x + \beta$, where $\alpha, \beta \in \mathbb{Z}_q^*$ for a large prime q. Let G be an additive group with prime order q. Also, let P be the generator of additive group G.

3.2 Registration Phase

In this phase, SP selects a random number $x_{sp} \in \mathbb{Z}_q^*$ as its secret key and computes $P_{sp} = x_{sp}P$ as its public key. Then, it selects a hash function $h(.) : \{0,1\}^* \rightarrow \{0,1\}^{160}$. Then, it selects a random number $x_i \in \mathbb{Z}_q^*$ as the secret key of each smart meter. Then SP stores (id_i, x_i) in its memory, and also saves $(id_i, x_i, P, h(.), q, P_{sp})$ in the memory of SM_i.

3.3 Authentication and Key Establishment Phase

An authentication between a smart meter (SM) and a service provider (SP) is done, where the details are described in what follows.

- **Step 1.** A single service provider selects $r \in \mathbb{Z}_q^*$, calculates $A_1 = rP$, retrieves time stamp T_1, and gives $M_1 = \{A_1, T_1\}$ to the smart meters in its coverage range.
- **Step 2.** The smart meter SM_i selects a random number $a \in \mathbb{Z}_q^*$, retrieves T_2, calculates $A_2 = aP$, $A_3 = aP_{sp}$, $A_4 = h(A_1, A_2, A_3, T_2)$, $A_5 = id_i \oplus A_4$ and $A_6 = h(id_i, A_1, x_i)$, and sends $M_2 = \{A_3, A_5, A_6, T_2\}$ to the SP.
- **Step 3.** The SP first checks the freshness of T_2. If it is fresh, SP obtains $A_2 = x_{sp}^{-1} A_3$, computes $A_4 = h(A_1, A_2, A_3, T_2)$ and then $id_i = A_5 \oplus A_4$. Next, SP checks if id_i exists in its database. If so, it finds x_i corresponding to id_i, calculates $A_6^* = h(id_i, A_1, x_i)$, and checks if A_6^* is equal to A_6. If the equality is not hold, SP rejects M_2; otherwise, SP retrieves T_3, calculates $A_7 = h(id_i, A_1, T_3)$, session key in form of $SK = h(A_2, A_4, T_1)$, and sends $M_3 = \{T_3, A_7\}$ to SM_i.
- **Step 4.** The smart meter SM_i checks the validity of T_3. If it is valid, SM_i calculates $A_7^* = h(id_i, A_1, T_3)$, and checks if $A_7^* \stackrel{?}{=} A_7$. If the equality holds, SP has been authenticated, and the session key is generated in the form of $SK = h(A_2, A_4, T_1)$.

4 Security Vulnerabilities of Sureshkumar *et al.*'s Scheme

In this section, it will be shown that Sureshkumar *et al.*'s scheme [9] is not forward secure, and it also suffers from stolen service provider database attacks. Moreover, we show that it is vulnerable against known session-specific temporary information attacks, as described below.

4.1 Lack of Forward Secrecy

This protocol does not support forward secrecy, while they claimed that it provides perfect forward secrecy in a way that if all long-term secret keys of entities are compromised, previous session keys remain secure and cannot be extracted. The details of this weakness are given below. If an adversary has secret key of SP, x_{sp}, can extract A_2 from A_3 with computing $A_2 = {x_{sp}}^{-1} A_3$, where A_3 is obtained from message M_2 on the public channel. Then, the adversary can compute $A_4 = h(A_1, A_2, A_3, T_2)$ since it gets A_1, A_3 and T_2 from the public channel. As a consequence, it can calculate the session key in form of $SK = h(A_2, A_4, T_1)$. Thus, Sureshkumar *et al.*'s scheme [9] cannot provide forward secrecy, and we show that with having the long-term secret key of just one entity, such as SP, the previous session keys are compromised.

4.2 Stolen Service Provider Database Attacks

In this attack, an adversary has access to the database of an SP and then threatens its security in a way that it can find secret keys, x_i of SM_i along with id_i, and can make smart meter impersonation attacks without being detected by SP, The session key is also extracted, where details of these vulnerabilities are described in the following section.

- The adversary with doing the stolen database attack of a typical service provider has access to (x_i, id_i) of each smart meter SM_i, then it can impersonate smart meters and does Step 2 of the main protocol in Subsection 3.3 in way that it chooses a random number $a \in \mathbb{Z}_q^*$, retrieves T_2, calculates $A_2 = aP$, $A_3 = aP_{sp}$, $A_4 = h(A_1, A_2, A_3, T_2)$, $A_5 = id_i \oplus A_4$ and $A_6 = h(id_i, A_1, x_i)$, and sends $M_2 = \{A_3, A_5, A_6, T_2\}$ to SP.
- Step 3 is the verification done by SP and is the same as Step 3 of the protocol as given in Subsection 3.3, and message M_2 will be passed since it has been generated based on the Step 2 of the protocol as explained before.
- After that, the adversary answers to SP similar to Step 4 of the protocol since it has (x_i, id_i). Consequently, the adversary can generate session key SK and can eavesdrop on exchanged messages between SM_i and SP.

4.3 Known Session-Specific Temporary Information Attacks

This protocol is not secure against known session-specific temporary attacks in a way that if ephemeral secret values at the user side, $A_2 = aP$, have been leaked, then the generated session keys are compromised. In this protocol, the session key SK is generated in the form of $SK = h(A_2, A_4, T_1)$, where A_2 is the only secret ephemeral value at the user side. Hence, if A_2 is known to the adversary, it first calculates $A_4 = h(A_1, A_2, A_3, T_2)$, and then computes $SK = h(A_2, A_4, T_1)$, where A_1, A_3, T_1 and T_4 are on the public channel.

5 Our Proposed Protocol

This section performs the following steps between the service provider (SP) and smart meters SM_i to create session keys for secure communications.

5.1 Setup

The service provider SP selects an elliptic curve $E(\alpha, \beta) : y^2 = x^3 + \alpha x + \beta$, where $\alpha, \beta \in \mathbb{Z}_q^*$ for a large prime q. Let G be an additive group with prime

order q. Also, let P be the generator of the additive group G.

5.2 Registration phase

In this phase, SP selects a random number $x_{sp} \in \mathbb{Z}_q^*$ as its secret key and computes $P_{sp} = x_{sp}P$ as its public key. Then, it selects a hash function $h(.) : \{0,1\}^* \rightarrow \{0,1\}^{160}$. Then, it selects a random number $x_i \in \mathbb{Z}_q^*$ as the secret key of each smart meter and computes $P_i = x_i P$ as their public keys, and also SP selects a random temporary string, RTS_i, a random number $K_i \in \mathbb{Z}_q^*$ and id_i for each SM_i, and calculates $PID_i = id_i \oplus h(K_i, RTS_i)$ and $EK_i = E_{x_{sp}}(K_i)$, where $E_{x_{sp}}(.)$ is symmetric encryption such as AES, where RTS_i is a random temporary string, K_i is used as the secret key of SP for the smart meter SM_i, and id_i is the identity of the SM_i. Then SP stores $(P_i, PID_i, RTS_i, EK_i)$ in its memory, and also saves $(id_i, x_i, P_i, RTS_i, P, h(.), q, P_{sp})$ in the memory of SM_i.

5.3 Login and Authentication Phase

- **Step 1.** The service provider SP selects a random number $r \in \mathbb{Z}_q^*$, computes $A_1 = rP$, and broadcasts $M_1 = \{A_1, T_1\}$ to all smart meters in their coverage range, where T_1 is the current time stamp.
- **Step 2.** The smart meter SM_i selects a random number $a \in \mathbb{Z}_q^*$, computes $A_2 = h(id_i, x_i A_1, RTS_i, T_2) \oplus aP_{sp}$ and $A_3 = h(aP, id_i, x_i A_1, T_2)$ and sends $M_2 = \{A_2, A_3, RTS_i, T_2\}$ to the service provider SP.
- **Step 3.** The service provider SP finds (P_i, PID_i, EK_i) corresponding to RTS_i, computes $K_i = D_{x_{sp}}(EK_i)$ and $id_i = PID_i \oplus h(K_i, P_i)$, and then computes $aP_{sp} = A_2 \oplus h(id_i, rP_i, RTS_i, T_2)$, $aP = x_{sp}^{-1} aP_{sp}$ and $A_3^* = h(aP, id_i, rP_i, T_2)$ and checks if $A_3^* \stackrel{?}{=} A_3$. If so, SP computes $SK = h(id_i, aP, rP_i, raP)$. Then, SP selects a new RTS_i^{new}, computes $A_4 = RTS_i^{new} \oplus h(RTS_i, id_i, aP_{sp}, T_3)$ and $A_5 = h(RTS_i^{new}, id_k, SK, aP, aP_{sp}, T_3)$, and sends $M_3 = \{A_4, A_5, T_3\}$ to SM_i.
- **Step 4.** The smart meter SM_i computes $RTS_i^{new} = A_4 \oplus h(RTS_i, id_i, aP_{sp}, T_3)$, $SK = h(id_i, aP, x_i A_1, aA_1)$ and computes $A_5^* = h(RTS_i^{new}, id_i, SK, aP, aP_{sp}, T_3)$, and checks if $A_5^* \stackrel{?}{=} A_5$. If so, then SM_i calculates $A_6 = h(RTS_i^{new}, aP_{sp}, T_4)$, and sends $M_4 = \{A_6, T_4\}$ to SP, and replaces RTS_i with RTS_i^{new}.
- **Step 5.** The SP computes $A_6^* = h(RTS_i^{new}, aP_{sp}, T_4)$, and examines if A_6^* is equal to A_6. If so, it confirms that the information on the smart meter side has been updated, and then it updates RTS_i, to RTS_i^{new}.

6 Security Analysis

6.1 Informal Aecurity Analysis

In this subsection, the security of the proposal is discussed below.

- **Resistance to the de-synchronization attacks (SR_1).** A protocol is said to be secure against de-synchronization attacks if some exchanged messages between entities are blocked by the adversary and the information cannot be updated on both sides. In our protocol, SP updates RTS_i in each session, and it is replaced with the new one when it gets the message M_4 indicating SM_i has updated RTS_i to RTS_i^{new}. If an adversary interrupts any messages, both sides will be affected. For instance, in Step 3 of Subsection 5 the new information related to SM_j at SP have been chosen and message M_3 is sent to SM_j, and in Step 4 of Subsection 5, SM_j gets this information and updates RTS_j^{new} if A_5 is valid and then sends A_6 as its confirmation of updating this value to SP. Therefore, our proposal is secure against de-synchronization attacks.
- **Smart meter anonymity (SR_2).** A protocol provides anonymity of smart meters if the identity of smart meters cannot be obtained from exchanged messages between SP and SMs. Our proposal satisfies this feature since the id_i is not in the exchanged messages, and the random number RTS_i is used on behalf of id_i. In addition, the value of id_i in SP's database is encrypted to be protected. As a consequence, the proposed protocol has smart meter anonymity.
- **Forward security (SR_3).** It is said that a protocol is forward secure if the previous session keys cannot be compromised when the long-term secret keys of all entities are leaked. In our protocol, the session key is $SK = h(id_i, aP, rP_i, raP)$, where the value of raP is obtained from aP and $A_1 = rP$, and its value is independent of the long-term secret keys of other entities. This value is changed in each session so that the session key will differ. Hence, our protocol provides forward secrecy.
- **Resistance to the known session-specific temporary information attacks (SR_4).** In this attack, the adversary knows remporary random values a and r, but it cannot generate the session key $SK = h(id_i, aP, rP_i, raP)$ since the value id_i is secret and is used in session key generation.
- **Resistance to the stolen service provider**

Table 2. Login and authentication phase of our protocol

Smart meter (SM_i)		Service provider (SP)
Generates a random number $a \in \mathbb{Z}_q^*$		
Retrieves T_2		
Computes		
$A_2 = h(id_i, x_i A_1, RTS_i, T_2) \oplus aP_{sp}$		
$A_3 = h(aP, id_i, x_i A_1, T_2)$		
$M_2 = \{A_2, A_3, RTS_i, T_2\}$	$\xrightarrow{M_2}$	
		Finds (P_i, PID_i, EK_i) corresponding to RTS_i
		Computes
		$K_i = D_{x_{sp}}(EK_i)$
		$id_i = PID_i \oplus h(K_i, P_i)$
		$aP_{sp} = A_2 \oplus h(id_i, rP_i, RTS_i, T_2)$
		$aP = x_{sp}^{-1} aP_{sp}$
		$A_3^* = h(aP, id_i, rP_i, T_2)$
		Checks if $A_3^* \stackrel{?}{=} A_3$
		If so, computes $SK = h(id_i, aP, rP_i, raP)$
		Selects a new RTS_i^{new}
		Retrieves T_3
		Computes $A_4 = RTS_i^{new} \oplus h(RTS_i, id_i, aP_{sp}, T_3)$
		$A_5 = h(RTS_i^{new}, id_i, SK, aP, aP_{sp}, T_3)$
		$M_3 = \{A_4, A_5, T_3\}$
	$\xleftarrow{M_3}$	
Computes		
$RTS_i^{new} = A_4 \oplus h(RTS_i, id_i, aP_{sp}, T_3)$		
$SK = h(id_i, aP, x_i A_1, aA_1)$		
$A_5^* = h(RTS_i^{new}, id_i, SK, aP, aP_{sp}, T_3)$		
Checks if $A_5^* \stackrel{?}{=} A_5$		
Retrieves T_4		
$A_6 = h(RTS_i^{new}, aP_{sp}, T_4)$		
$M_4 = \{A_6, T_4\}$		
Replaces RTS_i with RTS_i^{new}		
	$\xrightarrow{M_4}$	
		Computes
		$A_6^* = h(RTS_i^{new}, aP_{sp}, T_4)$
		Checks if $A_6^* \stackrel{?}{=} A_6$
		If so, replaces RTS_i with RTS_i^{new}

database attacks (SR_5). In this attack, an adversary can access the SP database and violate the protocol's security. In our protocol, stored information in SP's memory, such as id_i, is encrypted to be protected. In addition, the smart meter secret key is not stored in SP's database. As a consequence, the proposal provides security against authentication table leakage attacks.

- **Resistance to smart meter traceability attacks (SR_6).** In this attack, a smart meter SM_i can be traced from fixed parameters in exchanged messages. In our protocol, messages M_1, M_2, M_3 and M_4 are changed due to the use of random numbers during different sessions. For instance, in message M_2, the value a

is changed in each session, and also RTS_i is updated for the next session. Therefore, the adversary cannot find a connection between the two messages M_2 and M_2' in two different sessions.

- **Resistance to replay attacks (SR_7).** In this attack, by resending old messages, the adversary tries to login and authenticate itself without being detected by SP. In our protocol, for instance, in addition to employing time stamps, random numbers such as a and RTS_i are used, and these values are changed in each session. Consequently, if the adversary sends an old message, SP cannot accept it. As a consequence, the proposal is secure against replay attacks.
- **Smart meter impersonation attacks (SR_8).** In this attack, the adversary generates a valid message M_2 in a way that SP will accept it. In our protocol, for this goal, it has to compute a valid A_2, and so it needs to know x_i, id_i and RTS_i, but these values are dedicated to SM_i, and the adversary does not have these values. Therefore, the protocol is secure against impersonation attacks.

6.2 Formal Security Analysis

6.2.1 Security Analysis Using BAN Logic

The notations of BAN logic are summarized in Table 3.

Table 3. Notations of BAN logic

Notation	Description
$P \mid\equiv X$	*P believes X*
$P \mid\sim X$	*P once said X or P had sent message X*
$P \triangleleft X$	*P sees or receives X*
$P \overset{K}{\rightleftharpoons} X$	*The K is a secret formula which, can be used by P and X to prove their identity to another, because only P and X know the K*
$P \Rightarrow X$	*P has jurisdiction over X*
$\#(X)$	*X is fresh*
$\langle X \rangle_N$	*X is encrypted with N*
$P \overset{K}{\leftrightarrow} Q$	*K is a shared secret key between P and Q*

6.2.2 BAN Logic Rules

The following rules of BAN logic that is given in [31] are reviewed.

- R_1. Nonce verification rule: $\frac{P\mid\equiv\#(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
- R_2. Freshness conjuncatenation rule: $\frac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$
- R_3. Seeing rule: $\frac{P\triangleleft(X,Y)}{P\triangleleft X}$
- R_4. Message meaning rule: $\frac{P\mid\equiv P\overset{K}{\leftrightarrow}Q, P\triangleleft\{X\}_k}{P\mid\equiv Q\mid\sim X}$
- R_5. Belief 1: $\frac{P\mid\equiv Q\mid\equiv (X,Y)}{P\mid\equiv Q\mid\equiv X}$
- R_6. Belief 2: $\frac{P\mid\equiv Q\mid\sim(X,Y)}{P\mid\equiv Q\mid\sim X}$

6.2.3 Security Goals

In this subsection, security goals are required to be proved are given in what follows.
Goal 1. $SP \mid\equiv SM_i \mid\equiv aP$
Goal 2. $SM_i \mid\equiv SP \mid\sim (SK, RTS_i^{new})$
Goal 3. $SM_i \mid\equiv SP \mid\equiv \{RTS_i^{new}, SK\}$
Goal 4. $SP \mid\equiv SM_i \mid\equiv \{RTS_i^{new}\}$

6.2.4 Assumptions

In this section, we present the used assumptions in the proof of our protocol below.
$\mathbf{s_1}$: $SP \mid\equiv \#(aP, RTS_i, RTS_i^{new})$
$\mathbf{s_2}$: $SP \mid\equiv SM_i \overset{id_i}{\longleftrightarrow} SP$
$\mathbf{s_3}$: $SM_i \mid\equiv SM_i \overset{id_i}{\longleftrightarrow} SP$
$\mathbf{s_4}$: $SP \mid\equiv \#(T_2, T_4)$
$\mathbf{s_5}$: $SM_i \mid\equiv \#(T_3)$
$\mathbf{s_6}$: $SP \mid\equiv SM_i \overset{aP_{sp}}{\longleftrightarrow} SP$

6.2.5 Idealization

In this section we present an idealized form of our protocol as follows.
$SM_i \rightarrow SP : M_2 = \{l_1\}$
$l_1 : \{\langle aP, RTS_i, T_2\rangle_{id_i}\}$
$SP \rightarrow SM_i : M_3 = \{l_2, l_3\}$
$l_2 : \{\langle RTS_i^{new}, SK, aP, T_3\rangle_{id_i}\}$
$l_3 : \{\langle aP, T_3\rangle_{id_i}\}$
$SM_i \rightarrow SP\ M_4 = \{l_4\}$
$l_4 : \{\langle RTS_i^{new}, T_4\rangle_{aP_{sp}}\}$

6.2.6 Proof

In this subsection, the idealized version of our protocol, assumptions, and BAN logic rules are used to prove the aforementioned security goals.
According to M_2 and R_3 we have:
$P_1 : SP \triangleleft l_1$
Based on P_1, l_1, s_2, and R_4 we have:
$P_2 : SP \mid\equiv SM_i \mid\sim aP$ Based on P_2, s_1 and R_1 we have:
$P_3 : SP \mid\equiv SM_i \mid\equiv aP$ (*Goal* 1)
According to M_3 and R_3 we have:
$P_4 : SM_i \triangleleft l_2$
$P_5 : SM_i \triangleleft l_3$
According to P_4, l_2, s_3 and R_4 we have:
$P_6 : SM_i \mid\equiv SP \mid\sim \{RTS_i^{new}, SK\}$ (*Goal* 2)
According to P_6, s_5 and R_1 we have:
$P_7 : SM_i \mid\equiv SP \mid\equiv \{RTS_i^{new}, SK\}$ (*Goal* 3)
According to M_4 and R_3 we have:
$P_8 : SM_i \triangleleft l_4$
Based on l_4, s_6 and R_4 we have:
$P_9 : SP \mid\equiv SM_i \mid\sim RTS_i^{new}$

According to P_9, s_1 and R_1 we have:
$P_{10} : SP \mid\equiv SM_i \mid\equiv \{RTS_i^{new}, SK\}$ (*Goal* 4)

Consequently, fulfilling all goals *Goal* 1, *Goal* 2, *Goal* 3 and *Goal* 4 indicates the security of the session key.

6.3 Security Analysis using ProVerif

In this subsection, the security of our proposal is verified using ProVerif. Table 4 and Table 5 present queries and results, respectively. Furthermore, the results presented in Table 5 indicate that the authentication process between service providers and smart meters is successful, and the session key is secure.

7 Evaluation

In this section, an evaluation of our proposal and its comparison with related schemes in terms of security requirements, computation overhead and communication overhead is given.

7.1 Security Requirements Comparison

In Table 6, the security properties of our protocol are listed to be compared with other protocols [9–14, 22, 23]. In Table 6, SR_1 stands for resistance to desynchronization attack, SR_2 denotes the smart meter anonymity, SR_3 means forward security, SR_4 is used for resistance to the known session-specific temporary information attack, SR_5 stands for resistance to the stolen service provider database attack, SR_6 means resistance to smart meter traceability attack, SR_7 denotes resistance to replay attack, and SR_8 is used for resistance to smart meter impersonation attacks. As can be seen in Table 6, the existing protocols cannot resist different attacks, such as security against stolen authentication leakage attacks, smart meter impersonation attacks and resistance to the known session-specific temporary information attacks. In addition, some of them cannot provide perfect forward secrecy as claimed. As a consequence, our proposed protocol achieves more security features compared to baseline papers [9–12, 14, 22, 23].

7.2 Computation Overhead

In this subsection, a comparison of our protocol with related protocols in terms of computational cost at smart meters and service providers is given in Table 8. In the comparison, just the most time-consuming operations are considered. It should be noted in the computation comparison that only protocols that have forward secrecy and the anonymity of smart meters are considered. In Table 8, T_H, (T_E/T_D), T_M and T_b stand for the run-time of hash, symmetric encryption/decryption, scalar multiplication and bilinear pairing operation, respectively. It should be highlighted that the run-time of cryptographic operations [9, 14] is summarized in Table 7. As shown in Table 8, the computation cost of our scheme is increased compared to that of [9, 14], while it provides more security features than those. Furthermore, its computation cost is lower than other related schemes [10, 13, 22, 23].

7.3 Communication Cost

The communication cost of our protocol compared to schemes [9, 10, 13, 14, 22, 23], which support forward-secrecy and anonymity of smart meters, in terms of bits for smart meters and service providers are summarized in Table 9. In the comparison, it is assumed that the size of the hash value, an ECC point, the time stamp and an AES encryption/decryption scheme is 160 bits, 320 bits, 32 bits, and 128 bits, respectively. In addition, it is supposed that $|RTS_i|$= 40 bits. It should be noted that the communication overhead at a smart meter is the size of messages M_2 and M_4, where $M_2 = \{A_2, A_3, RTS_i, T_2\}$ and $M_4 = \{A_6, T_4\}$. Therefore, the communication cost at a smart meter is $|M_2|+|M_4|= |A_2|+|A_3|+|RTS_i|+|A_6|+|T_2|+|T_4|=$ 744 bits. Similarly, the communication cost at the service provider is the size of message M_3, where $M_3 = \{A_4, A_5, T_3\}$. As a consequence, the communication overhead at SP is $|M_3|= |A_4|+|A_5|+|T_3|=$ 352 bits. As seen from Table 9, our communication cost compared to the baseline paper [9] is increased, while our protocol provides more security features.

8 Conclusion

In this paper, we proved that the authenticated key establishment protocol presented by Sureshkumar *et al.* [9] in 2020 fails to provide forward secrecy and security against known-session-specific temporary information, stolen database of service providers and smart meter impersonation attacks. Then, a modified protocol was introduced to tackle the aforementioned vulnerabilities. Then, it is shown that it accomplishes session key security using BAN logic and ProVerif. In addition, we show that our protocol is secure by presenting an informal analysis. Eventually, a comparison of our protocol in terms of security features, communication and computation costs was presented, and it should be highlighted that it not only can provide more security requirements for smart grids but also has rational performance.

References

[1] J. Shao J. Song, Y. Liu and C. Tang. A dynamic membership data aggregation (dmda) protocol for smart grid. *IEEE Systems Journal*, 14(1):900–

Table 4. Queries

```
(*_____queries_____*)
query attacker (SK).
query attacker (Ki).
query attacker (xi).
query attacker (xsp).
query attacker (idi).
query attacker (idk).
query idi:bitstring; inj-event(endSM(idi)) ==> inj-event(beginSM(idi)).
query idk:bitstring; inj-event(endSP(idk)) ==> inj-event(beginSP(idk)).
(*|process|*)
process
    ((!SM)|(!SP))
```

Table 5. The result

```
Verification summary:
Query not attacker(SK[]) is true.
Query not attacker(Ki[]) is true.
Query not attacker(xi[]) is true.
Query not attacker(xsp[]) is true.
Query not attacker(idi[]) is true.
Query not attacker(idk[]) is true.
Query inj-event(endSM(idi_2)) ==> inj-event(beginSM(idi_2)) is true.
Query inj-event(endSP(idk_1)) ==> inj-event(beginSP(idk_1)) is true.
```

Table 6. Comparison of security features

Security features	[14]	[23]	[22]	[9]	[12]	[10]	[11]	[13]	Ours
SR_1	N	N	N	Y	Y	Y	Y	Y	Y
SR_2	Y	N	Y	Y	N	Y	N	Y	Y
SR_3	Y	Y	N	N	N	N	N	Y	Y
SR_4	Y	Y	N	N	N	N	N	Y	Y
SR_5	Y	Y	Y	N	Y	Y	Y	Y	Y
SR_6	N	Y	N	N	N	Y	N	Y	Y
SR_7	Y	Y	Y	N	Y	Y	Y	Y	Y
SR_8	Y	Y	Y	N	Y	Y	Y	Y	Y

Note: Y and N denote yes and no, respectively.

Table 7. Runtime of operations (ms) [9, 14]

T_H	T_E	T_D	T_M	T_b
0.001	0.003	0.004	0.27	3

908, 2020.

[2] N. Saxena and B. J. Choi. Integrated distributed authentication protocol for smart grid communications. *IEEE Systems Journal*, 12(3):2545–2556, 2018.

[3] P. Castillejo Y. Chen, J.-F. Martínez and L. López. An anonymous authentication and key establish scheme for smart grid: Fauth. *Energies 2017,*, 10(9):https://doi.org/10.3390/en10091354, 2017.

[4] H. Naqvi S. Kumari X. Li K. Mahmood, S. A. Chaudhry and A. K. Sangaiah. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81, 2018.

[5] M. Ashouri-Talouki A. Karampour and B. T. Ladani. Light-weight privacy-preserving data aggregation protocols in smart grid metering networks. *The ISC International Journal of Information Security (ISeCure)*, 14(3):101–112, 2022.

[6] W. Li D. Wang and P. Wang. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 14(9):4081–4092, 2018.

[7] D. Wang and P. Wang. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Transactions*

Table 8. Computation cost

protocol	Smart meter (SM_i)	Service provider (SP)	Total cost
Zhang *et al.* [14]	$7T_H + T_D$	$9T_H + T_D + 2T_E$	0.03
Odelu *et al.* [23]	$6T_H + 3T_M + T_E$	$6T_H + 2T_M + 2T_b + T_D$	7.369
Tsai and Lo [22]	$5T_H + 4T_M + T_E$	$5T_H + 3T_M + T_D + 2T_b$	8.983
Sureshkumar *et al.* [9]	$4T_H + 2T_M$	$4T_H + 2T_M$	1.088
Xia *et al.* [10]	$19T_M$	$18T_M$	9.99
Badar *et al.* [13]	$4T_H + 5T_M$	$8T_H + 9T_M$	3.792
Our protocol	$6T_H + 4T_M$	$7T_H + T_D + 3T_M$	1.907

Table 9. Communication cost in terms of bits

protocol	Smart meter (SM_i)	Service provider (SP)	Total cost
Zhang *et al.* [14]	448	288	736
Odelu *et al.* [23]	1120	480	1600
Tsai and Lo [22]	1120	480	1600
Sureshkumar *et al.* [9]	672	192	864
Xia *et al.* [10]	1504	1312	2816
Badar *et al.* [13]	1280	960	2240
Our protocol	744	352	1096

on Dependable and Secure Computing, 15(4):708–722, 2018.

[8] A. K. Das P. Singh S. Kumari M. Bayat, Z. Z. Jousheghani and M. R. Aref. A lightweight privacy-preserving authenticated key exchange scheme for smart grid communications. *The ISC International Journal of Information Security (ISeCure)*, 11(2):113–128, 2019.

[9] R. Amin N. Selvarajan V. Sureshkumar, S. Anandhi and R. Madhumathi. Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication. *IEEE Systems Journal*, 15(3):3565–3572, 2020.

[10] J. Wang Z. Xia, T. Liu and S. Chen. A secure and efficient authenticated key exchange scheme for smart grid. *Heliyon*, 9(7):e17240, 2023.

[11] B. Xing Z. Li Y. Guo D. Zhang X. Zhang D. He J. Zhang X. Yu W. Wang X. Huang S. Chai, H. Yin. Provably secure and lightweight authentication key agreement scheme for smart meters. *IEEE Transactions on Smart Grid*, 14(15):3816–3827, 2023.

[12] N. Egide and F. Li. Hap-sg: Heterogeneous authentication protocol for smart grid. *Peer-to-Peer Networking and Applications*, 16:1365–1379, 2023.

[13] W. Akram Z. Ghaffar M. Umar H. M. S. Badar, K. Mahmood and A. K. Das. Secure authentication protocol for home area network in smart grid-based smart cities. *Computers and Electrical Engineering*, 108(2023), 2023.

[14] S. Yin C.-H. Chi R. Liu L. Zhang, L. Zhao and Y. Zhang. A lightweight authentication scheme with privacy protection for smart grid communications. *Future Generation Computer Systems*, 100(18):770–778, 2019.

[15] M. Sain A. Martin P. Kumar, A. Gurtov and P. H. Ha. Lightweight authentication and key agreement for smart metering in smart energy networks. *IEEE Transactions on Smart Grid*, 10(4):4349–4359, 2019.

[16] P. Kumar A. Braeken and A. Martin. Efficient and provably secure key agreement for modern smart metering communications. *Energies*, 11(10):26–62, 2018.

[17] D.Wu and C. Zhou. Fault-tolerant and scalable key management for smart grid. *IEEE Transactions on Smart Grid*, 2(2):375–381, 2011.

[18] J. Xia and Y. Wang. Secure key distribution for the smart grid. *IEEE Transactions on Smart Grid*, 3(3):1437–1443, 2012.

[19] D. Wu and C. Zhou. Security weakness in the smart grid key distribution scheme proposed by xia and wang. *IEEE Transactions on Smart Grid*, 4(3):1613–1614, 2013.

[20] L. Zhu J. Zhang N. Liu, J. Chen and Y. He. A key management scheme for secure communications of advanced metering infrastructure in smart grid. *IEEE Transactions on Industrial Electronics*, 60(10):4746–4756, 2013.

[21] Y. Yang Z. Wan, G. Wang and S. Shi. Skm: Scalable key management for advanced metering infrastructure in smart grids. *IEEE Transactions on Industrial Electronics*, 61(12):7055–7066, 2014.

[22] J.-L. Tsai and N.-W. Lo. Secure anonymous key distribution scheme for smart grid. *IEEE Transactions on Smart Grid*, 7(2):906–914, 2016.

[23] M. Wazid V. Odelu, A. Kumar Das and M. Conti. Provably secure authenticated key agreement scheme for smart grid. *IEEE Transactions on Smart Grid*, 9(3):1900–1910, 2018.

[24] A. K. Das V. Odelu and A. Goswami. A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security*, 10(9):1953–1966, 2015.

[25] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *Proc. of Advances in Cryptology—EUROCRYPT 2001: International Con-*

ference on the Theory and Application of Cryptographic Technique, pages 453–474, Innsbruck, Austria, 6-10 May 2001. Springer-Verlag, Berlin.

[26] R. N. Akram C. Shepherd and K. Markantonakis. Establishing mutually trusted channels for remote sensing devices with trusted execution environments. In *Proc. of the 12th International Conference on Availability, Reliability and Security (ARES 2017)*, pages 1–10, Reggio Calabria, Italy, 29 August-1 September 2017. ACM.

[27] D. He D. Wang, H. Cheng and P. Wang. On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. *IEEE Systems Journal*, 12(1):916–925, 2018.

[28] J. Ni J. Ma X. Ma Q. Jiang, N. Zhang and K.-K. R. Choo. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transaction on Vehiculat Technology*, 69(9):9390–9401, 2020.

[29] P.Wang D.Wang and C.Wang. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in wsns. *ACM Transactions on Cyber-Physical Systems*, 4(3):1–26, 2020.

[30] M. S Obaidat V. Sureshkumar, R. Amin and I. Karthikeyan. An enhanced mutual authentication and key establishment protocol for tmis using chaotic map. *Journal of Information Security and Applications*, 53, 2020.

[31] R.M. Needham M. Burrows M, M. Abadi. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

Mustafa Husam Shareef Alrzij graduated in 2015 with a B.Sc. in Communication Systems Engineering from Iraq University College in Basra, Iraq. He is currently a M.Sc. student in Electrical Engineering from Science and Research Branch, Islamic Azad University. Enhancing Network Security in infrastructures is one of his research focuses.

Maryam Rajabzadeh Asaar received her B.Sc. degree in Electrical Engineering from Shahid Bahonar University of Kerman, Kerman, Iran, in 2004, and received her M.Sc. and Ph.D. degrees in Electrical Engineering from Sharif University of Technology, Tehran, Iran in 2008 and 2014, respectively. She is currently an assistant professor at Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran. Her research interests include Provable Security, Digital Signatures, Design and Analysis of Cryptographic Protocols and Network Security and Security in Industrial Control Systems.