frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 18 March 2025
DOI 10.3389/fphy.2025.1529638

OPEN ACCESS

EDITED BY
Francisco Welington Lima,
Federal University of Piauí, Brazil

REVIEWED BY
Azeem Irshad,
Govt. Graduate College Asghar Mall, Pakistan
Gladstone Alencar Alves,
Universidade Estadual do Piau, Brazil
Devishree Naidu,
Shri Ramdeobaba College of Engineering and Management, India
Akber Khan,
IIMT College of Engineering Greater Noida, India

*CORRESPONDENCE
Zhaoshun Wang,
zhswang@sohu.com

RECEIVED 17 November 2024
ACCEPTED 24 February 2025
PUBLISHED 18 March 2025

CITATION
Xiao N, Wang Z and Sun X (2025) A secure and efficient authentication scheme for vehicle to grid in smart grid.
Front. Phys. 13:1529638.
doi: 10.3389/fphy.2025.1529638

A secure and efficient authentication scheme for vehicle to grid in smart grid

Nan Xiao, Zhaoshun Wang* and Xiaoxue Sun

School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China

As environmental issues and climate change worsen, Smart Grid has become a crucial technology for tackling energy challenges. Smart Grid substantially enhances the reliability, security and efficiency of power systems by integrating state-of-the-art communication, control and information technologies. As a crucial component of Smart Grid, Vehicle to Grid (V2G) facilitates bidirectional energy flow between electric vehicle (EV) and the grid. This not only optimizes energy utilization but also accelerates the large-scale adoption of EV, contributing to a more sustainable energy ecosystem. However, security and privacy concerns in V2G cannot be ignored, particularly regarding identity authentication and data protection. Therefore, enabling the secure transmission of users' private information within V2G is crucial. This paper presents a secure and efficient authentication scheme for privacy preserving in V2G. The scheme validates vehicle user identities and leverages chebyshev chaotic maps along with hash function to enable V2G communication. It ensures both data integrity and user privacy during transmission, addressing key security concerns in V2G. Through formal security analysis, it is confirmed that the scheme can withstand common attacks. Additionally, detailed informal security discussions demonstrate that the scheme can resist known attacks and meet design objectives. Further performance evaluation shows that the proposed scheme balances efficiency and security.

KEYWORDS

smart grid, vehicle to grid, privacy preserving, authentication, security

1 Introduction

As awareness of environmental issues and climate change increases, concerns over fossil fuels and environmental pollution are also rising. Against this backdrop, traditional power grids can no longer meet the demands for energy security, economic efficiency, and environmental protection. As a result, Smart Grid has emerged [1], incorporating advanced communication, control and information technologies to enable monitoring, control and optimization of the power grid. These advancements enhance the grid's security and economic performance [2]. V2G refers to using electric vehicles (EVs) as energy storage and regulation devices that connect to the power grid, enabling the bidirectional flow of electricity, thereby enhancing energy utilization efficiency and cutting costs [3]. The significance of V2G technology stems from its ability to facilitate bidirectional energy flow and management. On one hand, during periods of lower demand, the surplus electricity can be directed to charge electric vehicle batteries, helping to avoid resource waste. On the other hand, when grid load is high, electric vehicles can return stored energy from their batteries

to the grid, thereby reducing pressure on the grid and improving its flexibility and stability [4]. Meanwhile, vehicle owners can use V2G technology to turn their electric vehicles into reliable energy storage devices and earn income. This new revenue stream can encourage more people to purchase electric vehicles, driving their widespread adoption [5]. Therefore, V2G in Smart Grid presents significant practical benefits and has wide-ranging potential applications.

V2G facilitates the bidirectional exchange of information and electricity between electric vehicles and the power grid, greatly improving the Smart Grid's operational efficiency. Nevertheless, V2G faces considerable challenges related to security and privacy concerns [6]. Prior to the power grid delivering services to electric vehicles, mutual authentication between the two parties is necessary. In the absence of such authentication, malicious actors may impersonate legitimate entities to gain access to the identity and location data of electric vehicle [7]. Moreover, since the communication takes place over public wireless networks, external attackers could intercept user information and compromise privacy for personal benefit [8]. If malicious attackers gain access to an electric vehicle's user identity data and vehicle information, they could deduce the vehicle's movement patterns based on charging and discharging locations and times, further inferring the user's life patterns, such as home address, workplace, social activities and when the user leaves home. Such privacy breaches pose threats to both the user's life and property [9]. V2G also involves payment processes during charging and discharging, which raises further security and privacy concerns for users. Therefore, dependable and secure mechanisms for privacy protection are essential in Smart Grid [10]. Authentication is a security mechanism used to confirm that an entity's identity is legitimate and genuine, aiming to ensure that only authorized entities can access protected resources, engage in communication, or perform specific operations [11–13]. In V2G environment, authentication is particularly important, as it prevents unauthorized access and tampering, ensuring the security of both information and systems, thus providing reliable services to EV users, aggregators and grid operators [14]. To prevent malicious attackers from impersonating legitimate entities in V2G communication and stealing users' private information, it is critical to develop a protocol that verifies the authenticity of the participants' identities and guarantees communication security within the V2G network. The key contributions are as follows:

1) This paper proposes a secure and efficient authentication scheme for V2G. First, the scheme verifies vehicle user identities, allowing users to participate in subsequent authentication and secure charging/discharging transactions only after successful login. In addition, the scheme employs the chebyshev chaotic maps algorithm and hash function to achieve lightweight V2G communication.
2) To evaluate the effectiveness and practicality of the proposed scheme, formal and informal security analysis are used to conduct an analysis. Through proof, the scheme achieves mutual authentication, data integrity, forward security and other essential security properties, successfully defending against typical security threats. Additionally, the proposed scheme balances security and efficiency, with performance analysis showing that it has advantages in resource consumption, meeting the scalability and efficiency demands of the Smart Grid.

The rest is organized as follows: Section 2 provides related work on V2G. Section 3 outlines the network and adversary models. Section 4 describes the design. Section 5 conducts a security analysis of the scheme. Section 6 presents the performance evaluation, and Section 7 summarizes the paper.

2 Literature review

V2G refers to a technology that facilitates two-way communication, enabling electric vehicles to serve not only as energy consumers but also as energy storage units capable of supplying power to the grid. However, security and privacy concerns for V2G have attracted considerable attention from researchers globally and domestically.

Wu et al. [15] introduced a management protocol that integrates symmetric key techniques with elliptic curve public key cryptography. This protocol offers benefits such as high scalability, and efficiency. However, Xia et al. [16] highlighted that the protocol is susceptible to man-in-the-middle attacks and suggested a trusted third-party-based authentication and key distribution protocol, which has been proven to defend against such attacks. Park et al. [17] noted that this approach relies entirely on the security of the underlying cryptographic algorithm and is incapable of resisting unknown key-sharing and impersonation attacks. Given the substantial data transmission required in vehicle-to-grid communications, Guo et al. [18] proposed a batch authentication protocol for V2G networks. However, this protocol is essentially a variation of the standard DSA algorithm and fails to ensure privacy protection for sensitive vehicle data or provide security against various network threats. Turkanovic [19] introduced an authentication protocol that provides password protection and supports the addition of dynamic nodes. Chang [20] highlighted several weaknesses in the protocol, including vulnerability to impersonation attacks, node capture, theft of smart devices, and spoofing of sensor nodes, as well as its failure to provide forward security. To address these issues, Chang et al. [20] introduced an authentication scheme using elliptic curve encryption that guarantees optimal forward security. However, the introduction of blockchain significantly increases the resource overhead of the protocol. To reduce authentication overhead, researchers both domestically and internationally have carried out a series of studies on lightweight authentication protocols. Wazid et al. [21] combined passwords, biometrics, and mobile devices to design a three-factor authentication protocol for V2G networks. Although the protocol achieves the goal of being lightweight, it fails to protect user privacy. However, it fails to provide user privacy protection. Shen et al. [22] introduced a lightweight authentication protocol designed for V2G networks. Although this protocol reduces computational overhead, it results in significant storage overhead due to the aggregation of vehicle authentication information.

Bansal et al. [23] introduced an authentication protocol utilizing physical unclonable functions. Ahmed et al. [24] developed a protocol using signcryption and unsigncryption techniques within a V2G communication setting based on the energy internet. Nevertheless, this protocol does not provide protection for vehicle data privacy and falls short in ensuring the forward security of session keys.

Chim et al. [25] introduced an electric vehicle authentication protocol that utilizes blind signatures. In this protocol, electric vehicles initially create a set of anonymous credentials, which are blindly signed by a trusted authority after verifying the vehicle's identity. These signed anonymous credentials can then be used by vehicles to search for, query, and reserve charging stations. However, the security of this protocol depends on a trusted authority to verify the vehicle's identity. If the authority is compromised or malicious, user privacy may not be adequately protected. Furthermore, this protocol only provides one-way authentication, with the authority authenticating the vehicle, which may lead to impersonation attacks. Chen et al. [26] proposed an authentication protocol, allowing charging/discharging stations to perform anonymous authentication and dynamic management of electric vehicles. However, the protocol suffers from high overhead in managing vehicle revocation. Yang et al. [27] used identity-based restrictive partially blind signature technology to construct a privacy-preserving authentication protocol, ensuring that verifiers cannot link the permits to the real identity of the electric vehicles. However, Wang et al. [28] highlighted that the reward system structure of the V2G network in protocol [27] lacks a formal security definition to capture real-world attacks. Wang et al. subsequently proposed a new traceable anonymous authentication protocol, which was proven secure in a formal security model. Saxena et al. [29] developed a two-factor authentication protocol, which relies on bilinear pairing technology. This method boosts the efficiency of authentication while preserving message integrity, ensuring forward privacy, and protecting identity anonymity. Nevertheless, the protocol lacks the capability to track the identities of malicious vehicles. Eiza et al. [30] employed certificateless public key encryption technology to construct a protocol, protecting the identity and location privacy of mobile electric vehicles. However, in this protocol, electric vehicles must interact with the server multiple times to verify their legitimacy, resulting in significant computational overhead. Gope et al. [31] proposed a protocol for V2G based on the energy internet, allowing charging and discharging at different geographically distributed charging stations. However, pseudonyms in this protocol do not provide complete anonymity, and semi-trusted service providers may collude with external attackers to gain users' privacy. To address this issue, Feng et al. [32] introduced an anonymous and traceable authentication protocol that incorporates a certificate blinding algorithm to protect user privacy. However, the protocol fails to ensure forward security and imposes significant computational burdens on the vehicle side. The existing framework struggles to balance efficiency and security, leading to potential risks in deployment. The provably secure and easy-to-deploy solution proposed in this paper provides technical support to address these pressing challenges and helps promote the large-scale application of V2G.

3 Preliminaries

3.1 Communication model

In our communication model, when the grid and electric vehicles engage in communication sessions, the electric vehicle needs to frequently report real-time information to the grid. Before joining the V2G network to submit information reports, EVs must undergo mutual authentication with local aggregators to ensure the accuracy and reliability of the reported information. In Figure 1, the communication model in this paper includes Trust Authority (TA), Aggregator (AGT) and Electric Vehicle (EV) [22–24].

TA is the cornerstone of the system, primarily responsible for generating system parameters, thereby ensuring the stable operation of the V2G network.

AGT plays the role of an information hub, responsible for collecting real-time status data from electric vehicles within its communication coverage area that wish to connect to the grid. The AGT is also tasked with verifying the legitimacy of EV identities, ensuring that only authenticated EV can participate in information exchange, thereby maintaining network security and ensuring data integrity.

EV must report a series of key data to the AGT in real-time, including but not limited to its battery level, charging location, battery type, battery capacity, and current charging status. This information is critical for grid scheduling and optimization. To achieve this, each EV is outfitted with an onboard unit (OBU) that serves as a communication device, enabling a secure and reliable link for communication with AGT.

3.2 Threat model

In the model, we define the foundational assumptions of system security. In this scheme, the channel between EV and AGT is assumed to be insecure and may be vulnerable to various forms of external attacks and interference. We assume that the TA is capable of defending against both known and unknown attacks, and its security and reliability are critical to the overall security of the system. In this model, AGT is considered a semi-trusted entity, meaning it strictly follows predefined protocols and processes, but may, out of curiosity or potential self-interest, attempt to exploit the information obtained during the authentication process. EV, on the other hand, is considered an untrusted entity. This assumption is based on the fact that EV may be produced by different manufacturers with varying levels of security and reliability, and there is a risk of the vehicle being manipulated by malicious users. Malicious EV may exploit the insecure channel to carry out a range of network attacks, including data tampering, replay attack, and so on, which would pose serious threats to the overall security and stability of the system [27–29].

3.3 Chebyshev chaotic maps

The Chebyshev chaotic maps do not require handling scalar multiplication in elliptic curves cryptography (ECC) or time-consuming modular exponentiation, offering high parallel

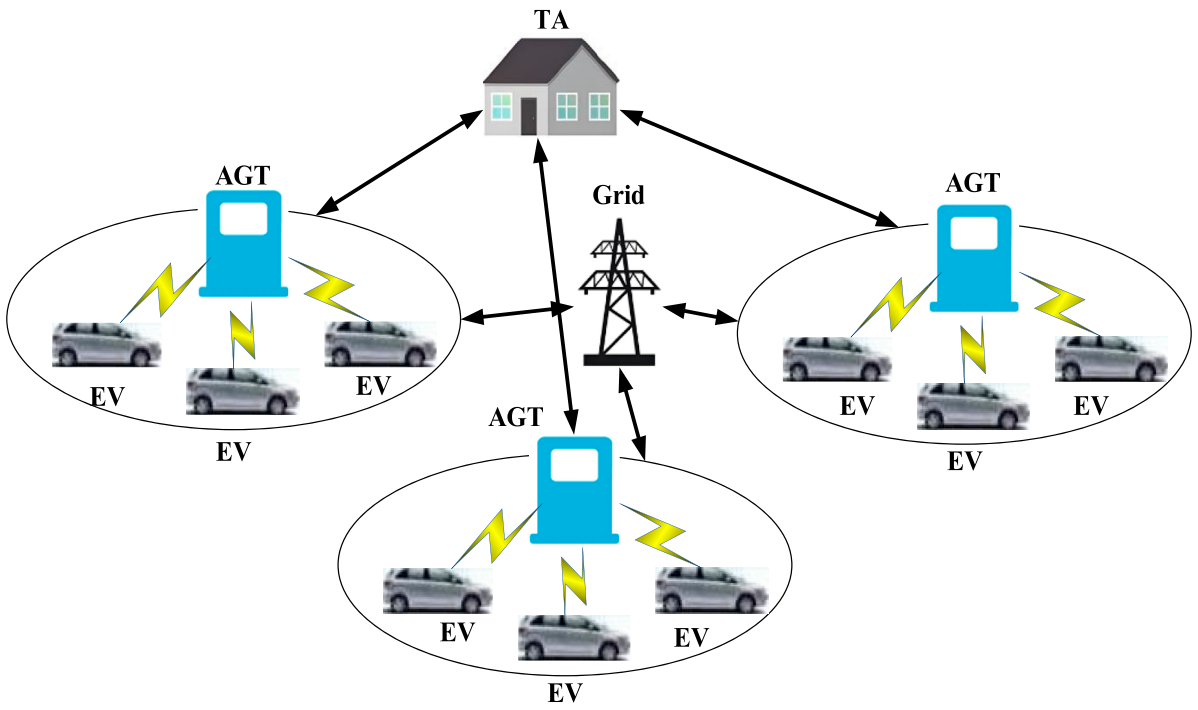

FIGURE 1
Communication Model of V2G System.

computational efficiency. Its lightweight nature makes it highly suitable for constructing authentication protocols in IoT application scenarios [33].

Definition 1: Define n as an integer and x within the interval $[-1, 1]$. The Chebyshev polynomial can be expressed either as Equations 1, 2:

$$T_n(x) = cos(n \cdot arccos(x)) \tag{1}$$

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)(modp) \tag{2}$$

Definition 2: (Semigroup Property): A key characteristic of Chebyshev polynomials is semigroup property. This property persists even when the domain of Chebyshev polynomials extends over the intervals $(-\infty, +\infty)$. An enhanced version is formulated as Equation 3:

$$T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x)(mod p) \tag{3}$$

Zhang [34] has shown the consistency of the semigroup property in Chebyshev polynomials.

Definition 3: (Chaotic Map-Based Discrete Logarithm Problem (CMDLP)): Given x and y, it is almost impossible to find the integer n, such that $T_n(x) = y(\mathrm{mod}\, p)$.

Definition 4: (Chaotic Map-Based Diffie-Hellman Problem (CMDHP)): For given x, $T_s(x)$, and $T_r(x)$, it is exceedingly difficult to ascertain $T_{rs}(x)$.

4 Proposed scheme

Since communication devices in the V2G environment operate in public settings, this scheme is designed to prevent privacy information from being leaked due to attacks. The scheme facilitates session key negotiation between the EV and the AGT based on chebyshev chaotic maps. Lightweight cryptographic operations are employed during the authentication process, reducing both communication and storage overhead. Table 1 shows the definitions of symbols used in the designed protocol.

4.1 System initialization phase

TA will perform the following operations: TA selects a random number x and a large prime number p. Then, TA chooses a one-way hash function h and random number s for the private key, then computes $P_{pub} = T_s(x)$. Subsequently, TA publishes the system parameters $\{h, x, p, P_{pub}\}$.

4.2 Registration phase

Step 1: EV_i generates its real identity information ID_i, password W_i and a random number a_i. It calculates $A_i = T_{a_i}(ID_i \| W_i)$, $EW_i = h(ID_i \| W_i \| a_i)$, and sends the registration request $\{A_i, a_i, ID_i, EW_i\}$ to TA.
Step 2: After receiving registration request, TA uses a random number b_i, the private key s and A_i to compute the pseudonym information $PID_i = ID_i \oplus h(A_i \| s)$ for the electric vehicle, as

TABLE 1 Notations.

Notations	Definitions
TA	Registration center
EV	Electric vehicle
AGT	Local aggregator
ID_i	EV real identity information
h	One-way hash function
PID_i, PID_j	Pseudonym information
s	System key
SK_{ij}, SK_{ji}	Session key
a_i, x_j, c_i, z_j	Random number
TS_1, TS_2, TS_3	Timestamp

well as $ES_i = h(PID_i \| s \| b_i \| h(ID_i \| s))$ and $EA_i = EW_i \oplus a_i \oplus ES_i$. TA then sends $\{EA_i, PID_i\}$ to the electric vehicle and stores the corresponding information table $\{\{PI\}D_i, A_i\}$ in its local memory for further communication.

Step 3: After receiving $\{\{PI\}D_i, A_i\}$, EV_i computes $ES_i = EA_i \oplus EW_i \oplus a_i$, $EB_i = h(ES_i \| PID_i \| EW_i)$, and $ED_i = ES_i \oplus EW_i$, as well as $AE_i = a_i \oplus h(ID_i \| W_i)$. It then stores $\{PID_i, AE_i, \mathrm{EB}_i, ED_i\}$ locally.

The aggregator AGT_j also needs to be securely registered with the TA. AGT_j selects its real identity information ID_j and a random number x_j, calculates $X_j = T_{x_j}(ID_j \| x_j)$, and sends $\{ID_j, X_j\}$ to the registration center. TA generates a pseudonym information $PID_j = ID_j \oplus h(X_j \| s)$ and $AX_j = T_{x_j}(ID_j \| x_j) \oplus h(PID_j \| \mathrm{s})$. After registration, TA stores the information table $\{PID_j, X_j\}$ locally and sends $\{PID_j, AX_j\}$ to AGT_j. AGT_j generates a random number r_j, calculates $R_j = T_{r_j}(x)$, and broadcasts the pseudonym information PID_j along with R_j.

4.3 Login phase

To successfully initiate the electric vehicle, the user must input the password and identity information ID_i and password W_i. The system computes EW_i, ES_i, EB_i' and verifies whether $EB_i' = EB_i$ holds true. The calculation steps are shown in the following Formulas 4–7:

$$a_i = AE_i \oplus h(ID_i \| W_i) \tag{4}$$

$$EW_i = h(ID_i \| W_i \| a_i) \tag{5}$$

$$ES_i = ED_i \oplus EW_i \tag{6}$$

$$EB_i' = h(ES_i \| PID_i \| EW_i) \tag{7}$$

4.4 Authentication phase

Figure 2 shows the detailed authentication process.

Step 1: EV_i randomly chooses c_i and a timestamp TS_1. EV_i generates $EC_i = T_{c_i}(x)$, $ETA_i = T_{c_i}(P_{pub})$ and $EPR_i = h(PID_i \| ETA_i TS_1)$. It then calculates $A_i = T_{a_i}(ID_i \| W_i)$, $EI_i = h(ID_i \| TS_1 \| ETA_i)$, $EG_i = EPR_i \oplus EI_i$, $EID_i = EI_i \oplus PID_i$ and $EM_i = h(PID_i \| EI_i \| A_i \| TS_1)$. Finally, EV_i obtains PID_j and R_j from the broadcast channel. EV_i sends the authentication request $\{EID_i, PID_j, EG_i, EC_i, EM_i, TS_1\}$ to TA.

Step 2: On receiving $\{EID_i, PID_j, EG_i, EC_i, EM_i, TS_1\}$, TA verifies the validity of TS_1. If the threshold is exceeded, the authentication process is terminated. TA computes $ETA_i = T_s(EC_i)$, $EPR_i = h(PID_i \| ETA_i TS_1)$, $EI_i = EPR_i \oplus EG_i$ and $PID_i = EI_i \oplus EID_i$. TA then checks the local database to see if PID_i and PID_j exist. If the identities are found, it retrieves A_i and X_j. To verify the legitimacy of EV_i, TA computes $EM_i' = h(PID_i \| EI_i \| A_i \| TS_1)$ and checks if $EM_i' = EM_i$. If verified, TA selects the current timestamp TS_2, computes $TR_j = T_s(R_j)$, $TX_j = h(PID_j \| TR_j TS_2) \oplus h(PID_j \| \mathrm{s})$, $TM_j = h(PID_j \| TS_2 \| TR_j \| X_j)$ and sends $\{EC_i, TX_j, TM_j, TS_2\}$ to AGT_j.

Step 3: Upon receiving the message, AGT_j verifies the validity of TS_2. If the timestamp exceeds the threshold, the message is discarded. Otherwise, AGT_j computes $TR_j = T_{r_j}(P_{pub})$, $ATX_j = h(PID_j \| TR_j TS_2) \oplus TX_j$, and $X_j = ATX_j \oplus AX_j$. Then, $TM_j' = h(PID_j \| TS_2 \| TR_j \| X_j)$ is calculated to verify if $TM_j' = TM_j$. If $TM_j' = TM_j$, AGT_j selects a random number z_j and a timestamp TS_3, calculates $AZ_j = T_{z_j}(\mathrm{x})$, $AE_j = T_{z_j}(EC_i)$, the session key $SK_{ji} = h(PID_j \| AE_j \| TS_3)$ and the verification message $AEM_j = h(SK_{ij} \| TS_3 \| PID_j)$. The message $\{AEM_j, AZ_j, TS_3\}$ is then sent to V_i.

Step 4: On receiving $\{AEM_j, AZ_j, TS_3\}$, EV_i checks TS_3. If it is valid, EV_i computes $AE_i = T_{c_i}(AZ_j)$, the session key $SK_{ij} = h(PID_j \| AE_i \| TS_3)$, and the verification message $\mathrm{AEM}_i' = h(SK_{ij} \| TS_3 \| PID_j)$. If $\mathrm{AEM}_i' = AEM_j$, it proves that $SK_{ij} = SK_{ji}$. At this point, EV_i and AGT_j have successfully established a session key. If any step in the verification process fails, the protocol is terminated.

5 Security analysis of the protocol

5.1 Formal security analysis

The security model [28,34–39] will be introduced in detail below.

Definition 3.1: (Participant): Let EV_i^a, AGT_j^b, and TA^c denote the a-th instance of electric vehicle EV_i, the b-th instance of local aggregator AGT_j^b, and the c-th instance of the TA, respectively.

Definition 3.2: (Partnership): All transmitted information has a session identifier (SID). Instances EV_i^a and AGT_j^b are considered partners if they satisfy the following four conditions:

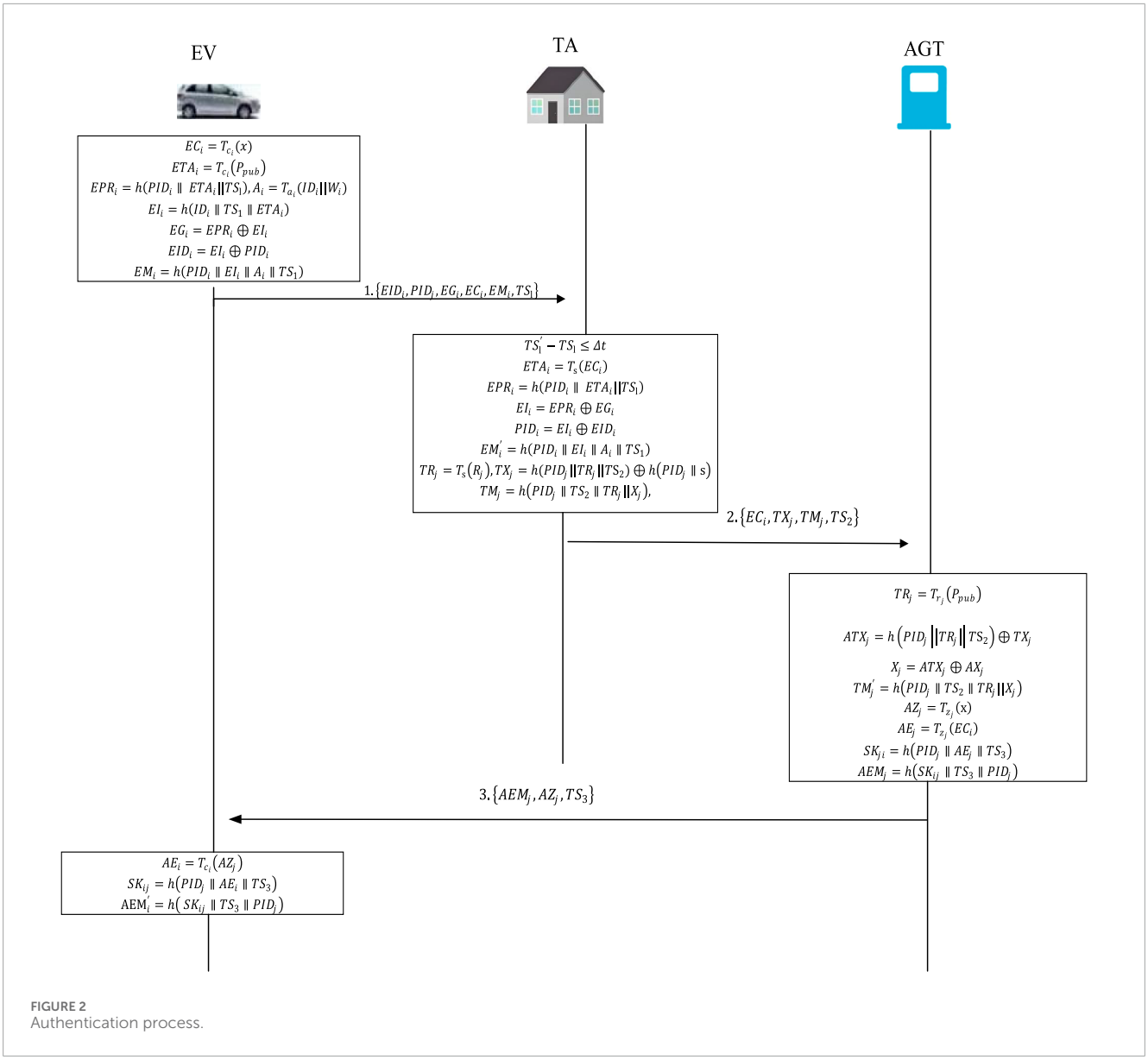

FIGURE 2
Authentication process.

(1) Both EV_i^a and AGT_j^b are in the accepted state;
(2) EV_i^a and AGT_j^b share the same *SID*;
(3) The partner identifier of EV_i^a is AGT_j^b, and the partner identifier of AGT_j^b is EV_i^a;
(4) No other instance is in the receiving state with the same partner identifier as EV_i^a or AGT_j^b.

Definition 3.3: (Freshness):

If the session key *SK* remains confidential between instances EV_i^a and AGT_j^b, and has not been disclosed to adversary A, then the session is regarded as fresh. It is hypothesized that adversary $\mathcal{A}$ has control over all communication exchanges between entities. Consequently, adversary $\mathcal{A}$ is able to conduct the following queries:

- $Execute\left(EV_i^a, AGT_j^b, TA^c\right)$: The adversary $\mathcal{A}$ can obtain all the information transmitted between the legitimate entities EV_i, AGT_j, and *TA*.
- $Send\left(EV_i^a, AGT_i^b, M\right)$: The adversary $\mathcal{A}$ sends message M to either instance EV_i^a or AGT_i^b, and the participant computes the protocol result and returns it to the adversary $\mathcal{A}$.
- $Reveal\left(EV_i^a, AGT_j^b\right)$: If a session key *SK* has been established between instances EV_i^a and AGT_j^b, the established session key is sent to the adversary $\mathcal{A}$. Otherwise, the answer is $\perp$ (meaning no established session key exists).
- $Corrupt\left(EV_i^a, AGT_j^b\right)$: The adversary can obtain the secret information from the instances EV_i^a and AGT_j^b in *Corrupt*.
- $Test\left(EV_i^a, AGT_j^b\right)$: It is used to verify the semantic security of the session key. Before executing *Test*, a coin b is flipped. If $b = 1$, the session key is sent to the adversary $\mathcal{A}$. If $b = 0$, a random number is returned as the answer. After this query is executed, if no session key *SK* has been established or if the session between EV_i^a and AGT_j^b is not fresh, $\perp$ is returned to the adversary $\mathcal{A}$.

Theorem 1: Assume that adversary $\mathcal{A}$ operates in the model and attacks the proposed scheme in polynomial time. The advantage of adversary $\mathcal{A}$ in breaking the session key security is defined as follows:

$$\mathrm{Adv}_{\mathcal{P},\mathcal{A}}^{AKA}(\mathcal{A}) \le \frac{q_H^2}{|hash|} + 2q_s\mathrm{Adv}_{\mathcal{P},\mathcal{A}}^{CMDHP}(t) \tag{8}$$

Here, q_h, q_{Send}, and $|Hash|$ represent hash query, send query and the size of the hash function output, respectively. $\mathrm{Adv}_{\mathcal{P},\mathcal{A}}^{CMDHP}(t)$ denotes the advantage of $\mathcal{A}$ in solving the CMDHP problem within polynomial time t.

Proof: The proof process is as follows:

- Game GM_0: This game simulates the actual attack initiated by the adversary, so we can express:

$$\mathrm{Adv}_{p}^{AKA}(\mathcal{A}) = \mid 2\Pr[Succ_0]\text{-}1 \mid \tag{9}$$

- Game GM_1: GM_1 simulates all the queries from GM_0. In addition, it simulates an eavesdropping attack performed by adversary $\mathcal{A}$. After the game, adversary $\mathcal{A}$ performs *Execute*. Adversary $\mathcal{A}$ must distinguish whether the output of the *Test* is the real session key or a random value. Since the final session key is generated as $SK_{ij} = h(PID_j \| AE_i \| TS_3)$, which includes the secret value AE_i, adversary $\mathcal{A}$ cannot obtain this secret value via eavesdropping within polynomial time. Hence, adversary A's probability of winning does not increase, meaning that the probabilities in games GM_0 and GM_1 are identical:

$$\Pr[Succ_1] = \Pr[Succ_0] \tag{10}$$

- Game GM_2: GM_2 simulates all the queries from GM_1 and adds Send query and hash query, thus modeling active attacks by adversary $\mathcal{A}$. In this game, the adversary's goal is to deceive participants into accepting modified messages. Adversary $\mathcal{A}$ can also perform different hash queries to find collisions. Since the transmitted information in the channel, such as $\{EID_i, PID_j, EG_i, EC_i, EM_i, TS_1\}$, $\{EC_i, TX_j, TM_j, TS_2\}$, $\{AEM_j, AZ_j, TS_3\}$, includes identity information, timestamps, nonces, and secret values, adversary $\mathcal{A}$ will not generate collisions during *Send* query. Based on the birthday paradox, we obtain:

$$|\Pr[Succ_2] - \Pr[Succ_1]| \le \frac{q_H^2}{2|Hash|} \tag{11}$$

- Game GM_3: All queries are simulated in GM_3. Suppose adversary $\mathcal{A}$ attempts to compute the session key $SK_{ij} = h(PID_j \| AE_i \| TS_3)$. Even if $\mathcal{A}$ performs Corrupt query in the game to obtain information, it must calculate $T_{z_j c_i}(\mathrm{x})$ based on $AZ_j = T_{z_j}(\mathrm{x})$ and $EC_i = T_{c_i}(x)$. It can be shown that adversary $\mathcal{A}$ can solve the CMDHP problem within polynomial time t. Hence, it has:

$$|\Pr[Succ_3] - \Pr[Succ_2]| \le q_s\mathrm{Adv}_{\mathcal{P},\mathcal{A}}^{CMDHP}(t) \tag{12}$$

In GM_3, adversary $\mathcal{A}$ performs the *Test* query and guesses the bit b to win the game. It has

$$\Pr[Succ_3] = \frac{1}{2} \tag{13}$$

Finally, by combining the results from Equations (8)–(13), it has

$$\mathrm{Adv}_{\mathcal{P},\mathcal{A}}^{AKA}(\mathcal{A}) \le \frac{q_H^2}{|hash|} + 2q_s\mathrm{Adv}_{\mathcal{P},\mathcal{A}}^{CMDHP}(t) \tag{14}$$

5.2 Informal security analysis

Informal security analysis of the security protocol is used to evaluate the protocol's security and correctness, aiming to identify potential security risks and vulnerabilities [27,40–43]. The security of the protocol is described informally in this paper, demonstrating that the designed protocol satisfies the security, and can resist impersonation attack, replay attack and other potential threats.

5.2.1 Mutual authentication

Upon receiving the message $\{EID_i, PID_j, EG_i, EC_i, EM_i, TS_1\}$ from the electric vehicle EV_i, the TA verifies whether $EM_i' = h(PID_i \| EI_i \| A_i \| TS_1)$ matches EM_i. If $EM_i' \neq EM_i$, the TA terminates the session. If $EM_i' = EM_i$, the TA considers EV_i a legitimate user. After receiving the message $\{EC_i, TX_j, TM_j, TS_2\}$ from TA, AGT_j verifies whether $TM_j' = h(PID_j \| TS_2 \| TR_j \| X_j) = TM_j$. If valid, AGT_j considers TA legitimate. When EV_i receives the message $\{AEM_j, AZ_j, TS_3\}$ from AGT_j, it verifies whether $\mathrm{AEM}_i' = h(SK_{ij} \| TS_3 \| PID_j) = AEM_j$. If they match, EV_i considers AGT_j legitimate. Therefore, the scheme ensures mutual authentication.

5.2.2 Unlinkability

Each time communication occurs, EV_i identity information is transmitted in encrypted form, and the associated authentication information is calculated using random numbers and timestamps. Therefore, each encrypted identity and authentication message is independent, with no linkable information between them. As a result, external attackers cannot determine whether two or more messages originate from the same sender, demonstrating that the scheme satisfies unlinkability.

5.2.3 Conditional privacy protection and traceability

In the proposed protocol, the vehicle only transmits its real identity information to the registration center during the registration phase. Upon receiving the user's registration request, the registration center uses its private key to compute a pseudonym $PID_i = ID_i \oplus h(A_i \| s)$, which is then sent to the user as the identity for subsequent communication. Throughout the entire protocol, the user's real identity information is not revealed, ensuring conditional privacy protection. Furthermore, since the pseudonym is generated using the registration center's private key, any malicious vehicle in the V2G environment can be traced by the registration center. TA can trace a malicious vehicle by locating its pseudonym, retrieving A_i from the local database, and using the private key to compute $ID_i = PID_i \oplus h(A_i \| s)$, thus revealing the vehicle's real identity.

5.2.4 Forward security

After successful mutual authentication between EV_i and AGT_j, a temporary session key $SK_{ij} = h(PID_j \| AE_i \| TS_3)$ is established. This session key is related to the random numbers z_j or c_i selected. Even if a previous session key is compromised, earlier session keys remain secure due to the uniqueness of the random numbers in each session. Thus, the proposed protocol ensures forward security.

5.2.5 Session key security

Only legitimate EV_i and AGT_j will negotiate a session key $SK_{ij} = h(PID_j \| AE_i \| TS_3)$ for communication after the authentication process is completed. Since the adversary cannot solve the CMDHP within polynomial time t, AE_i remains unrecoverable by the adversary. Additionally, the timestamp TS_3 included in the session key ensures the security of the session. If the session key is leaked, the adversary will not be able to use it to recover previous or future session keys.

5.2.6 Resistance to impersonation attack

The adversary attempts to impersonate a legitimate vehicle EV_i or aggregator AGT_j. In this attack, the adversary tries to masquerade as a legitimate entity by altering the authentication information they send. If successful, the adversary would gain unauthorized access to network resources. To successfully impersonate a legitimate vehicle, the adversary would need to compute the correct EM_i and send it to the registration center for verification. However, since $EM_i = h(PID_i \| EI_i \| A_i \| TS_1)$ includes EI_i, which requires the secret value c_i only known to the legitimate vehicle, it is not feasible for the adversary to forge a legitimate vehicle. Similarly, if the adversary attempts to impersonate an aggregator, they would also need to obtain the secret value z_j, without which they cannot pass the vehicle's verification of AEM_j.

5.2.7 Resistance to man-in-the-middle attack

Even if an adversary attempts to act as a man-in-the-middle and establish a connection with both legitimate parties, they cannot negotiate a session key with either party because they lack valid authentication credentials and cannot pass the verification process. Due to the complexity of the CMDHP, the adversary cannot forge valid authentication credentials, making the protocol resistant to man-in-the-middle attack.

5.2.8 Resistance to replay attack

All transmitted messages $\{EID_i, PID_j, EG_i, EC_i, EM_i, TS_1\}$, $\{EC_i, TX_j, TM_j, TS_2\}$, and $\{AEM_j, AZ_j, TS_3\}$ include timestamps $\{TS_1, TS_2, TS_3\}$ representing the freshness of the information. Upon receiving these messages, the recipient only needs to verify the freshness of the timestamps to determine whether a replay attack has occurred. In summary, the proposed scheme resists replay attack.

6 Performance analysis

6.1 Computational overhead

In this part of the paper, we assess the computational overhead associated with the proposed scheme. Fundamental operations in this scheme include ECC operations, bilinear pairing operations, and chaotic mapping operations. Similar to existing scheme, this evaluation focuses on high-cost computations. The computation overhead is primarily evaluated based on ECC operations, bilinear pairing operations, and chaotic map operations.

TABLE 2 Time consumption of basic operations (ms).

Notations	Description	Time
T_{pair}	Bilinear pairing	6.36
T_{a-bp}	Addition operation in bilinear pairing	0.012
T_{m-bp}	Multiplication operation in bilinear pairing	3.89
T_{m-ecc}	Multiplication operation in ECC	2.23
T_{a-ecc}	Addition operation in ECC	0.27
T_c	Chaotic map operation	1.14

TABLE 3 Comparison of computational overhead.

Protocol	Total computation overhead
[28]	$18T_{pair} + 17T_{m-bp} + 7T_{a-bp}$
[39]	$9T_{m-ecc} + 5T_{a-ecc}$
[27]	$12T_{pair} + 7T_{m-bp} + 3T_{a-bp}$
Our scheme	$9T_c$

Table 2 lists the time consumption of each cryptographic operation used in the scheme. Let T_{pair} be the time required for a single bilinear pairing operation, T_{a-bp} for an addition operation in bilinear pairing, T_{m-bp} for a multiplication operation in bilinear pairing, $T_{m-\mathrm{ecc}}$ for a multiplication operation in elliptic curves cryptography (ECC), $T_{a-\mathrm{sec}}$ for an addition operation in ECC, and T_c for a chaotic mapping operation. The experiments were conducted in a hardware environment consisting of 64-bit Windows 11, 16 GB of RAM, and the JPBC library.

We selected three similar schemes for comparison with our scheme. Table 3 displays the basic operations within each scheme. Figure 3 shows the computational overhead comparison for the authentication process of a single EV in the four schemes. In the authentication process, proposed scheme shows notable benefits in computational overhead when compared to other schemes.

6.2 Communication overhead

In this part, it is assumed that the output length of the hash function is 20 bytes, while the output of identity information and chaotic mapping are 20 bytes and 40 bytes, respectively. Additionally, during the authentication process, the output lengths of ECC, bilinear pairing, and the timestamp are 40 bytes, 64 bytes and 4 bytes, respectively. Based on the above, We evaluated the communication overhead of the proposed scheme.

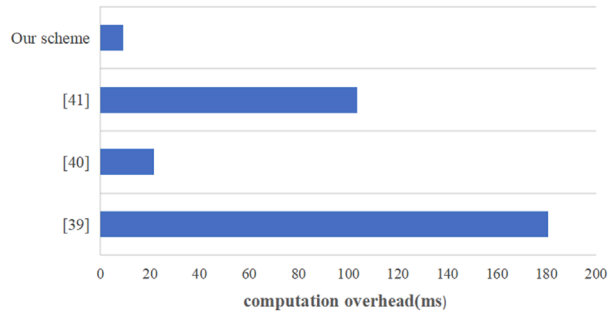

FIGURE 3
Computation overhead.

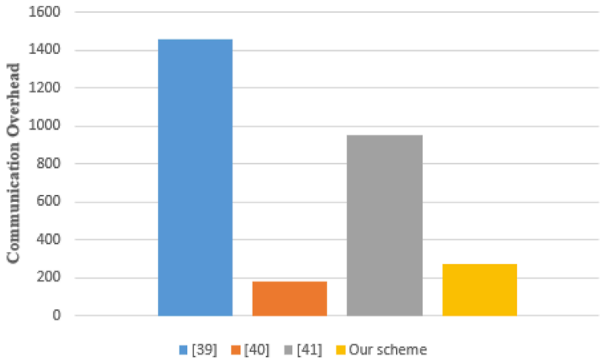

FIGURE 4
Communication overhead.

TABLE 4 Comparison of the communication Overhead.

Protocol	Communication overhead
[28]	1456
[39]	184
[27]	956
Our scheme	272

Table 4 compares the communication overhead during authentication for each scheme. The communication overhead of [28] is 1456 bytes. In [39], two messages are exchanged, resulting in a communication overhead of 184 bytes. In [27], the communication overhead is 956 bytes. In our scheme, the EV sends one message to the TA, the TA sends one message to the AGT, and the AGT sends one message to the EV. Overall, the total communication overhead of the proposed scheme is 272 bytes. Figure 4 shows a comparison during authentication for each scheme. The communication overhead of our scheme is significantly lower than [27,28], while it is slightly higher than [39]. However [39], does not satisfy traceability and forward security. Overall, while the proposed scheme is slightly less efficient in terms of communication compared to [39], it provides more comprehensive security features. As a result, our scheme demonstrates better overall performance.

7 Conclusion

V2G integrates smart grids with electric vehicles, allowing EV fleets to serve as energy storage units that buffer the grid and renewable energy, thereby reducing the costs associated with power generation infrastructure and leveraging electric vehicles to address environmental concerns. However, the wireless communication network in V2G is an open network, making it susceptible to various types of network attacks, posing a range of threats to EV users. The secure and efficient V2G authentication scheme proposed in this paper, through rigorous vehicle user identity verification mechanisms combined with chaotic mapping technology, effectively resists malicious attacks, ensuring the authenticity of identities and the integrity of data during V2G communication. The performance analysis demonstrates that the scheme performs excellently regarding overhead. This scheme not only provides essential security guarantees but also contributes to the development of green energy. In the future, as smart grid and electric vehicle technologies continue to advance, the scheme proposed in this paper can contribute to building a secure, efficient, and sustainable energy ecosystem.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

NX: Conceptualization, Formal Analysis, Validation, Writing–original draft, Writing–review and editing. ZW: Conceptualization, Formal Analysis, Validation, Writing–original draft. XS: Formal Analysis, Validation, Writing–original draft.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

References

1. Khalid M. Smart grids and renewable energy systems: perspectives and grid integration challenges. *Energ Strategy Rev* (2024) 51:101299. doi:10.1016/j.esr.2024.101299

2. Olatunde TM, Okwandu AC, Akande DO, Sikhakhane ZQ. The impact of smart grids on energy efficiency: a comprehensive review. *Eng Sci and Technol J* (2024) 5(4):1257–69. doi:10.51594/estj.v5i4.1016

3. Panchanathan S, Vishnuram P, Rajamanickam N, Bajaj M, Blazek V, Prokop L, et al. A comprehensive review of the bidirectional converter topologies for the vehicle-to-grid system. *Energies* (2023) 16(5):2503. doi:10.3390/en16052503

4. Mastoi MS, Zhuang S, Munir HM, Haris M, Hassan M, Alqarni M, et al. A study of charging-dispatch strategies and vehicle-to-grid technologies for electric vehicles in distribution networks. *Energ Rep* (2023), 9 1777–806. doi:10.1016/j.egyr.2022.12.139

5. Alsharif A, Ahmed AA, Khaleel MM, Alarga ASD, Jomah OSM, Imbayah I. Comprehensive state-of-the-art of vehicle-to-grid technology[C]. In: *2023 IEEE 3rd international maghreb meeting of the conference on sciences and techniques of automatic control and computer engineering (MI-STA)*. IEEE (2023). p. 530–4.

6. Yu S, Park K. PUF-based robust and anonymous authentication and key establishment scheme for V2G networks. *IEEE Internet Things J* (2024) 11(9):15450–64. doi:10.1109/jiot.2024.3349689

7. Novak A, Ivanov A. Network security vulnerabilities in smart vehicle-to-grid systems identifying threats and proposing robust countermeasures. *J Artif Intelligence Machine Learn Management* (2023) 7(1):48–80. doi:10.1109/ICOIN48656.2020.9016538

8. Itoo S, Som LK, Ahmad M, Baksh R, Masoodi FS. A robust ECC-based authentication framework for energy internet (EI)-based vehicle to grid communication system. *Vehicular Commun* (2023), 41. doi:10.1016/j.vehcom.2023.100612

9. Shamshad S, Mahmood K, Shamshad U, Hussain I, Hussain S, Das AK. A provably secure and lightweight access control protocol for EI-based vehicle to grid environment. *IEEE Internet Things J* (2023) 10(18):16650–7. doi:10.1109/jiot.2023.3269150

10. He S, Lin F, Zhao Y, Xiao Y, Tang W, Zhang F. *Design of multi-layer information security protection scheme for vehicle-to-grid system[C]//2023 3rd international conference on computer science, electronic information engineering and intelligent control technology (CEI)*. IEEE (2023). 77–82.

11. Miao J, Wang Z, Wu Z, Ning X, Tiwari P. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. *Expert Syst Appl* (2024) 237:121329. doi:10.1016/j.eswa.2023.121329

12. Shao H, Ma Y, Shao B. A lightweight privacy-preserving authentication scheme for vehicle-to-grid[C]. In: *2024 6th asia energy and electrical engineering symposium (AEEES)*. IEEE (2024). p. 278–82.

13. Xiao N. J. A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. *Alexandria Eng J* (2024) 86:631–43. doi:10.1016/j.aej.2023.12.021

14. Reddy AG, Babu PR, Odelu V, Wang L, Ap Kumar S. V2G-Auth: lightweight authentication and key agreement protocol for V2G environment leveraging physically unclonable functions. *IEEE Trans Ind Cyber-Physical Syst* (2023) 1:66–78. doi:10.1109/ticps.2023.3290539

15. Wu D, Zhou C. Fault-tolerant and scalable key management for smart grid. *IEEE Trans Smart Grid* (2011) 2(2):375–81. doi:10.1109/tsg.2011.2120634

16. Xia J, Wang Y. Secure key distribution for the smart grid. *IEEE Trans Smart Grid* (2012) 3(3):1437–43. doi:10.1109/tsg.2012.2199141

17. Park JH, Kim M, Kwon D. Security weakness in the smart grid key distribution scheme proposed by Xia and Wang. *IEEE Trans Smart Grid* (2013) 4(3):1613–4. doi:10.1109/TSG.2013.2258823

18. Guo H, Wu Y, Bao F, Chen H, Ma M. UBAPV2G: a unique batch authentication protocol for vehicle-to-grid communications. *IEEE Trans Smart Grid* (2011) 2(4):707–14. doi:10.1109/tsg.2011.2168243

19. Turkanovic M, Brumen B, Holbl M. A novel user authentication and key agreement scheme for heterogeneous *ad hoc* wireless sensor networks based on the internet of things notion. *Ad Hoc Networks* (2014) 20:96–112. doi:10.1016/j.adhoc.2014.03.009

20. Chang C, Le H. A provably secure efficient and flexible authentication scheme for *ad hoc* wireless sensor networks. *IEEE Trans Wireless Commun* (2016) 15(1):357–66. doi:10.1109/twc.2015.2473165

21. Wazid M, Das AK, Kumar N, Rodrigues JJPC. Secure three factor user authentication scheme for renewable-energy-based smart grid environment. *IEEE Trans Ind Inform* (2017) 13(6):3144–53. doi:10.1109/tii.2017.2732999

22. Shen J, Zhou T, Wei F, Sun X, Xiang Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things. *IEEE Internet Things J* (2018) 5(4):2526–36. doi:10.1109/jiot.2017.2775248

23. Bansal G, Naren N, Chamola V, Sikdar B, Kumar N, Guizani M. Lightweight mutual authentication protocol for V2G using physical unclonable function. *IEEE Trans Vehicular Technol* (2020) 69(7):7234–46. doi:10.1109/tvt.2020.2976960

24. Ahmed S, Shamshad S, Ghaffar Z, Mahmood K, Kumar N, Parizi RM, et al. Signcryption based authenticated and key exchange protocol for EI-based V2G environment. *IEEE Trans Smart Grid* (2021) 12(6):5290–8. doi:10.1109/tsg.2021.3102156

25. Chim T, Cheung J, Yiu S, Hui L, Li V. SPCS: secure and privacy-preserving charging-station searching using VANET. *J Inf Security* (2012) 3(1):59–67. doi:10.4236/jis.2012.31007

26. Chen J, Zhang Y, Su W. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-grid (V2G) networks. *China Commun* (2015) 12(3):9–19. doi:10.1109/cc.2015.7084359

27. Yang Z, Yu S, Lou W, Liu C. P^2: privacy-preserving communication and precise reward architecture for V2G networks in smart grid. *IEEE Trans Smart Grid* (2011) 2(4):697–706. doi:10.1109/tsg.2011.2140343

28. Wang H, Qin B, Wu Q, Xu L, Domingo-Ferrer J. TPP: traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids. *IEEE Trans Inf Forensics and Security* (2015) 10(11):2340–51. doi:10.1109/tifs.2015.2455513

29. Saxena N, Choi BJ. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks. *IEEE Trans Inf Forensics and Security* (2016) 11(7):1438–52. doi:10.1109/tifs.2016.2532840

30. Eiza MH, Shi Q, Marnerides A, Owens T. Secure and privacy-aware proxy mobile IPv6 protocol for vehicle-to-grid networks. In: *Proceedings of the 2016 IEEE international conference on communications (ICC)*. Malaysia: Kuala Lumpur (2016). p. 1938–883.

31. Gope P, Sikdar B. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Trans Smart Grid* (2019) 10(6):6607–18. doi:10.1109/tsg.2019.2908698

32. Feng X, Shi Q, Xie Q, Wang L. P2BA: a privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular *ad hoc* networks. *IEEE Trans Inf Forensics and Security* (2021) 16:3888–99. doi:10.1109/tifs.2021.3098971

33. Chen R, Mou Y, Li W. A provably secure multi-server authentication scheme based on Chebyshev chaotic map. *J Inf Security Appl* (2024) 83:103788. doi:10.1016/j.jisa.2024.103788

34. Zhang L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos, Solitons and Fractals* (2008) 37(3):669–74. doi:10.1016/j.chaos.2006.09.047

35. Parameswarath RP, Gope P, Sikdar B. A privacy-preserving authenticated key exchange protocol for V2G communications using SSI. *IEEE Trans Vehicular Technol* (2023) 72(11):14771–16. doi:10.1109/tvt.2023.3281371

36. Pandey R, Koranga M, Thakur SN. Securing vehicle-to-grid communications: a cyber-physical approach[m]//optimized energy management strategies for electric vehicles. *IGI Glob Scientific Publishing* (2025) 301–18. doi:10.1109/TSG.2013.2258823

37. Miao J, Wang Z, Ning X, Shankar A, Maple C, Rodrigues JJPC. A UAV-assisted authentication protocol for internet of vehicles. *IEEE Trans Intell Transportation Syst* (2024) 25(8):10286–97. doi:10.1109/tits.2024.3360251

38. Khan AA, Kumar V, Ahmad M, Jangirala S. A secure and energy efficient key agreement framework for vehicle-grid system. *J Inf Security Appl* (2022) 68:103231. doi:10.1016/j.jisa.2022.103231

39. Su Y, Shen G, Zhang M. A novel privacy-preserving authentication scheme for V2G networks. *IEEE Syst J* (2019) 1–9. doi:10.1109/TIFS.2015.2455513

40. Khan AA, Kumar V, Prasad R, Idrisi MJ. SGAK: a robust ECC based authenticated key exchange protocol for smart grid networks. *IEEE Access* (2024) 12:195745–59. doi:10.1109/access.2024.3434532

41. Shen J, Zhou T, Wei F, Sun X, Xiang Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things. *IEEE Internet things J* (2017) 5(4):2526–36. doi:10.1109/jiot.2017.2775248

42. Miao J, Wang Z, Wang M, Garg S, Hossain MS, Rodrigues JJ. Secure and efficient communication approaches for Industry 5.0 in edge computing. *Computer Networks* (2024) 242:110244. doi:10.1016/j.comnet.2024.110244

43. Iqbal A, Khan AA, Kumar V, et al. A mutual authentication and key agreement protocol for vehicle to grid technology[C]//Innovations. In: *Electrical and electronic engineering: proceedings of ICEEE 2021*. Singapore: Springer (2021). p. 863–75.