sTrade: Blockchain based Secure Energy Trading using Vehicle-to-Grid Mutual Authentication in Smart Transportation

Giriraj Sharma, Amit M. Joshi[a,1], Saraju P. Mohanty[b]

[a]*Dept. of Electronics & communication, MNIT, Malaviya Nagar, Jaipur, 302017, Rajasthan, India*
[b]*Dept. of comp science & Engg,University of North Texas, 1155 Union Cir, Denton, 76203, TX, USA*

Abstract

Electric vehicles are gaining popularity in the Vehicle-to-Grid network due to recharge batteries during off-peak electricity hours and discharge during peak hours. It allows for accomplishing electricity requirements in periods of high demand and additional storage in case of surplus generation from the grid. Electric vehicles also earn reward points for energy trading. The significant trading data volume processed by the underlying Vehicle-to-Grid infrastructure results in numerous security, privacy and scalability challenges. Researchers suggested various energy trading schemes but suffered from anonymity, large overheads, and dependency on a centralized system, which may cause single-point failure. As a solution, new design principles are desirable to enable the next generation of Vehicle-to-Grid networks. Decentralized energy information networks are a crucial aspect of future power grids, and blockchain technology offers promising potential to support local energy trading and decentralized power generation. Thus, a proposed framework uses the blockchain-based decentralized, secure, and privacy vehicle-to-grid network mutual authentication and energy trading system using elliptic curve cryptography with a scheduling feature.
The Proposed scheme is divided into four steps 1) Registration, 2) Scheduling, 3) Mutual authentication and 4) Consensus and energy trading. Distributed ledger blockchain technology makes every transaction valid and authentic, possibly minimizing or eliminating mediators in energy trading, while lightweight elliptical curve cryptography is used for mutual authentication. Further, the performance of our scheme is justified by using the popular AVISPA simulation tool. Our analysis illustrates that the proposed model is secure, privacy-preserving, and supports minimal communicational and computational overhead of 1750 bits and 7.027 ms compared to state-of-the-art work.

Keywords: Smart Transportation, Vehicle to Grid, Blockchain, Smart Grid, Mutual Authentication, Internet-of-Things (IoT)

1. Introduction

In the past few decades, conventional power grids are facing challenges of long-distance transmission, energy crisis, and carbon emission [1]. Efficient energy generation and utilization are necessary to make a clean and green environment [2]. Electric Vehicles (EVs) play a very important role in smart transportation because of their multiple advantages, such as reducing peak energy demand by discharge to the grid during electricity peak hours and charging from the grid during off-peak hours [3]. It would lead to less peak generating capacity and reduces carbon emission. At the same time, EVs get reward points for participating in energy trading. The cost of electricity is higher during the peak hours and lower during slack hours [4]. The vital advantage of V2G is that individual EVs may participate in energy trading without building any transmission network. Due to the mobility of EVs, intelligent and secure energy trading is a major challenge in the V2G network [5].

Recently, many researchers have suggested mutual authentication (MA) and cyber-physical security schemes based on cryptography for V2G, but these schemes have the drawback of single-point failure. V2G networks increasingly use IoT devices for automation monitoring and load control tasks. In the future, V2G and G2V will be aggregated with Internet-of-Things (IoT) to make the whole infrastructure smoother for smart transportation with V2G technology.
A blockchain is a decentralized and open distributed ledger and P2P data storage technique that uses hash values and timestamps to keep data safe and secure. Blockchain technology administers the recorded transactions between two entities securely and efficiently. As one of the most vital parts of the blockchain, the consensus mechanism is the core technology that enables distributed nodes to agree on the new block waiting to be published to the blockchain. It is crucial in maintaining trust between distrustful entities, such as EVs. It ensures fault-tolerance in agreeing on the same state of the blockchain network, such as a unified representation of all transactions in a cryptocurrency blockchain [6]. The application of blockchain technology in smart gird is advanced metering infrastructure, cyber-physical system, microgrid, smart transportation and V2G etc.
Thus, the proposed scheme devised a combination of blockchain and ECC for anonymous, secure, and efficient energy trading in the V2G network. The traditional authentication method uses a trusted third party, the main reason for single-point failure [7]. Therefore, our scheme uses blockchain

technology based on the decentralized concept with distributed global ledger features. The advantage of decentralisation is that it improves efficiency and security.

1.1. Contribution of the current paper

The motivation and novel research contributions of the proposed scheme are as follows:-

1.1.1. Motivation

1) The energy trading of V2G tends to rise with the rapid growth of EVs. It has increased security concerns and privacy issues such as false data injection, denial of service attacks, and integrity risks [8].

2) Most existing V2G energy trading schemes predominantly emphasize centralized solutions, which are susceptible to single-point failures along with associated vulnerabilities.

3) During energy trading time, EV owners have to wait a longer time, which requires to have proper scheduling mechanism.

4) Various e-MSP schemes are available that need to be integrated with blockchain for better security and transparent transaction [9] [10].

5) The novel sTrade scheme is developed using the PBFT blockchain and ECC-based mutual authentication for secure energy trading.

1.1.2. Research contribution

The major contributions of this paper are as follows

1) The network and adversary energy trading model is designed for smart transportation in the V2G network.

2) A secure framework for V2G energy trading is designed that supports public blockchain technology and ECC. In this scheme, the blockchain distributed ledger is leveraged for transaction execution in V2G, while ECC is employed for mutual authentication. The utilization of public blockchain further strengthens the network security of V2G transactions, ensuring a robust and trustworthy system.

3) The proposed scheme designed a mutual authentication scheme to prevent the identity of EVs. Hence, apart from e-MSP, no other entity knows the identity of EV.

4) Novel CS scheduling algorithm is implemented to reduce the waiting time. Hence, a minimum waiting time is required for charging or discharging.

5) The proposed scheme has validated the performance through a widely acceptable AVISPA tool. The proposed model is secure, privacy-preserving, and supports minimal communicational overhead.

The paper has been organized as follows: Section 2 covers the related literature on the energy trading of the V2G network while section 3 elaborates on research methodologies and energy trading model for the proposed system. Section 4 explains the security analysis, performance comparison and results of the proposed method. Section 5 concludes the work. The notations used in the current paper have been presented in Table 1.

Table 1: Notations used in the Current Paper

Abbreviation	Descriptions
ECC	Elliptical curve cryptography
EV	Electric vehicle
CS	Charging station
PoAh	Proof of authentication
GS	Grid server
G2V	Grid to vehicle
TTP	Trusted third party
PoW	Proof of work
P2P	Peer to Peer
e-MSP	Electric mobility service provider
CSMS	Charging station management system
EVSE	Electric vehicle supply equipment
PBFT	Practical BFT
PoA	Proof of activity
PoS	Proof of stake
DoS	Denial of service
V2G	Vehicle to grid
IDev, IDcs	ID EV, CS
PIDev, PIDcs	Pseudo ID of EV,CS
Tev, Tcs	Time stamp EV, CS
SKev, SKcs	Pvt key of EV,CS
PKev, PKcs	Public key of EV,CS
r1, r2	Random numbers
Authcs,Authev	Authentication message

2. Related work in Blockchain-based V2G Network

The V2G technology has shown substantial growth over the years across the world. Many researchers have suggested V2G energy trading scheme based on blockchain and mutual authentication. Table 2 presents a broad overview of the state-of-the-art.

Scheme [19] introduced a P2P energy trading scheme that facilitates transactions between EVs and e-MSP, aimed at managing demand response in a V2G environment. The researchers employed a double auction mechanism and a consortium blockchain in their proposed scheme. However, it was noted that the system's internal communication lacked anonymity, which could potentially lead to significant privacy violations.

Further[20] described a smart contract-based blockchain for energy trading between EVs and CSs without involving any trusted third party. However, this scheme is only feasible for a small number of EVs. Similarly, author [21] proposed blockchain technology to implement a privacy-preserving model for EVs and CSs. Scheme [22] suggested a secure and authenticated key exchange scheme that supports privacy and session-key security. The work demonstrated in paper [21] claimed that the scheme in [22] did not fulfil the anonymity condition of EVs and also suffered large computational overheads. [23] designed a security framework for V2G networks that incorporates ECC-based lightweight authentication and a privacy-preserving model. In this approach, EVs generate

Table 2: A comparative analysis of sTrade with different popular schemes

Scheme	Primitive used	Description
Li, et al. 2017 [11]	Consortium blockchain technology	No need of trusted third party in P2P energy trading, To overcome the transaction limitation credit payment scheme is adopted
Puthal et al. 2018 [12]	Proof of authentication (PoAh), Blockchains in the Internet of Things	Author claim that PoAh can replace existing consensus algorithms, such as PoS, PoW, and PoA for resource-constrained infrastructures, such as the IoT.
Gope, et al. 2019 [13]	XOR, hash function	High computational overhead, EVs identity not secure
Hassija, et al. 2020 [14]	Directed Acyclic Graph-based V2G network on DLT blockchain	Game theory model for negotiating in energy trading
Wang. et al 2021 [15]	Blockchain, ECC, batch verification	Need of strength the security in communication processes
Arpna, et al. 2022 [16]	Blockchain, Smart contract, machine learning	Suffers from EVs owner privacy and latency
Wazid, et al. 2022 [17]	Public blockchain, PBFT	Suggested a public blockchain-based secure communication model for intelligent transportation.
Wang, et al. 2023 [18]	Hashgraph-based block alliance Consensus	No scheduling and incentive mechanism for participants.
Proposed (sTrade)	PBFT Blockchain, Hash, ECC	Support electric mobility service (e-MSP), V2G energy trading, ECC based mutual authentication, scheduling and Identity privacy of EV.

random identification to protect their confidential information and ensure network security and confidentiality.

Further, the scheme in paper [24] offered a physical and cyber securities model. Recently [25], and [26] proposed mutual authentication between EV and CS, based on a blockchain using ECC, which were attempted to secure mutual authentication using ECC and blockchain technology. However, it suffered from high computational overheads, and there was no concept of EV scheduling [27]. Scheme [12] designed an IoT-based blockchain for EV and other devices.

Similarly, [14] scheme suggested a directed acyclic graph-based V2G network using DLT blockchain and game theory for negotiating in energy trading. Scheme [15] emphasized a blockchain and ECC-based batch verification protocol, but it lacks security in communication processes. Blockchain concept was used in LNSC lightning network scheme [28]. In this scheme, blockchain worked as TTP (Lightning network concept) instead of SP or utility centre, and MA was performed using the ECC technique without any SP. This scheme uses the scheduling concept, but it suffers from computational complexity. Scheme [16] suggested a V2G energy trading using machine learning, but this scheme suffered from EV privacy and latency. Recently scheme [18] designed a hashgraph-based block alliance consensus mechanism (BAC) but suffered from scheduling and incentive mechanisms for motivating participants. Similarly, scheme [29] elaborated a secure ECC and blockchain-based MA and energy trading network to handle the above-discussed issue.

The scheme [17] proposed a secure communication framework for intelligent transportation that utilizes a public blockchain. This scheme used the PBFT consensus mechanism for node selection. Similarly, scheme [18] described a hashgraph-based block alliance consensus for energy trading. Both schemes suffer from scheduling and electric mobility concepts. From the above literature review, it has been concluded that no scheme provides a complete solution for MA in V2G using blockchain for smart transportation.

3. Research Methodologies

3.1. Model of the Proposed V2G System

A blockchain based energy trading framework for V2G network is depicted in Fig.1. This system model comprises four main components EVSE, CSMS, e-MSP, and the blockchain network. The data of the blockchain network is transparent and unchangeable. The intruder or hacker can not alter the blockchain data as cryptographic hash primitives secure the information. The following section describes the function and role of each entity involved in the system:

1) Electric Vehicle (EV) :

EV is an important component of V2G system. It plays a crucial role due to its bi-directional energy trading capability. EVs can play a role as energy producers, discharging their batteries to provide electricity during peak times and charging them during off-peak hours as energy consumers. EVs can adjust their

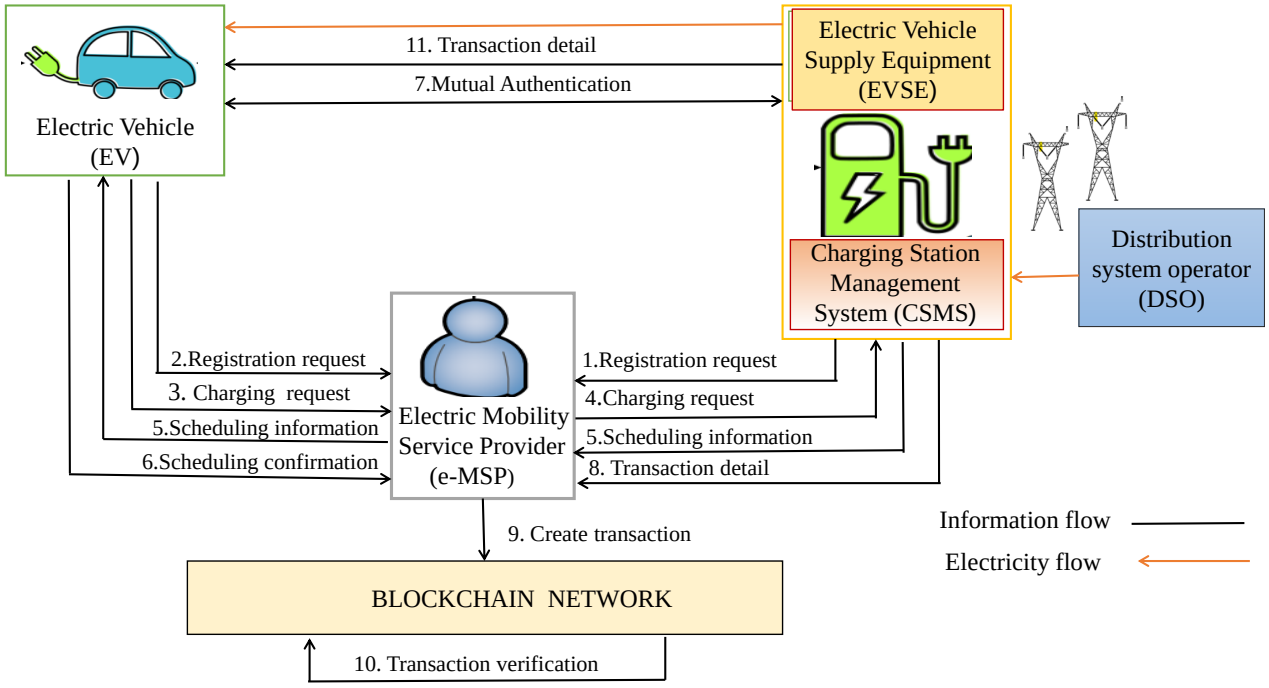

Figure 1: Overall process diagram of the proposed framework

charging and discharging behaviour dynamically through active participation in V2G energy trading to maximize their benefits. This two-way energy flow between EVs and the grid enables V2G services, where EVs contribute electricity to the grid and receive energy from the grid during peak times. Moreover, the blockchain network provides the incentive to EVs with reward points for their active participation in energy trading, promoting further adoption of V2G technologies.

2) Electric Vehicle Supply Equipment (EVSE):
The EVSE is a primary component of the CS and acts as the interface that connects EV to the charging station. It functions as the main system of the charging system, gathering data related to the EV's charging progress and connectivity status.

3) Charging Station (CS) :
The CS manages the EVSE and power connectors of EV. The CSMS controls the CS. EVs are charged and discharged at CS. EV sends the request to e-MSP for charging or discharging. e-MSP sends scheduling information to EV in consultation with CS.

4) Charging Station Management System (CSMS):
The CSMS serves as a central administrator of an EV charging system. Its main responsibilities include: (a) communicating with the CS and EVSE, (b) defining the parameters of the charging service based on user input, as well as considering the status of the EV and the power grid, and (c) collecting and storing data related to the charging system.

5) Distribution System Operator (DSO):
The DSO is a system administrator accountable for distributing electricity to customers. The DSO has the authority to permit or restrict power flow to charging sites and uses EV feedback to maintain grid balance and alleviate congestion [30].

6) Electric Mobility Service Provider (e-MSP):
The e-MSP is responsible for overseeing the economic aspects of the EV charging service. This includes issuing contracts on a per EV or per EV driver basis, as well as managing the billing processes associated with the charging service. e-MSP is a central authority that validates and maintains transactions between EV and CS in the blockchain.

7) Blockchain Network :
Integrating public blockchain technology into the proposed V2G energy trading security framework enhances its security, reliability, and decentralization. This is possible because to update transactions within a block in the blockchain, an adversary would need to modify the previous hash of all transactions and the elliptic curve primitives on the block. These verifications ensure that the block is authentic and no transactions have been tampered with by adversaries. Consequently, while the transactions or information within the blocks are public, adversaries cannot alter, delete, or modify them, thereby enhancing the security of smart transportation through blockchain technology [31]. Blockchain technology is applied to prove the transactions generated by the e-MSP between EVs and CSs. It also sends reward points to EV in a secure way.

3.2. Proposed Blockchain based V2G Framework

The blockchain-based secure V2G energy trading framework for smart transportation systems (sTrade) is described in this section. Once all the steps of sTrade are executed, the framework establishes access control mechanisms for data exchange

among EVs, e-MSP and CSMS. Integrating blockchain technology enhances the framework's security, reliability, and decentralization, essential requirements for smart energy trading.

sTrade consists of the following phases: a) Registration, b) Scheduling, c) Mutual authentication, and d) Consensus and block writing, discussed in detail below. It is considered that the clocks of the communicating entities are synchronized, which is a common assumption in the design of various authentication protocols for networking environments [17] [16] [9].

3.2.1. Registration process

The charging phase components are EV, CS, and e-MSP which need to be registered before the commencement of energy trading, t Registration of various components is performed in offline mode through a secure channel. Registration of different components is discussed below.

Step 1: In the initial step, the EV sends its IDev to the e-MSP; subsequently, it verifies whether the information of the EV is available in the blockchain. If IDev is unavailable earlier, the SP considers the EV's request and generates its public-private key pairs, i.e., SKev and PKev = SKev.P, and sent to the EV over a secure channel.

Step 2: CS is registered by sending their IDcs, and SKcs and public-private key pairs PKcs=SKcs.P are sent to CS.

3.2.2. Scheduling process

In this phase, EV sends the charging request to e-MSP by sending corresponding IDev and IDcs. After that e-MSP checks the IDs, verifies, searches nearby CSs, and sends information with EV location details. Schedules are prepared according to the demand of EV drivers and smart contracts.

The following parameters are considered while preparing the schedule:

(1) Distance from CS: The distance of EV with CS is calculated, and the minimum distance value Dsp is selected.

(2) Waiting time at CS: The waiting time Twt is calculated, and the minimum waiting time value Dwt is selected.

(3) Comprehensive cost: The total cost includes consumption cost (Wc) and time cost(t). The Dcc parameter is calculated at Wc*t.

(4) Time cost: The time cost value is calculated on the expected time to arrive at CS etc.

After receiving a request from CS, the scheduled values are calculated and sent to e-MSP for further transmission to EV. Msd =(Dsp ||Dwt ||Dcc ||Dtc). After receiving Msd, the EV confirms the charging request by sending a message (IDev||Tev) to the corresponding CS via e-MSP.

3.2.3. Mutual Authentication process

After arriving at CS, EV plugged in the charging station socket. EVs and CS mutually authenticate before any energy trading. The authentication message combines ECC keys, hash function, and concatenation operations.

Step 1: In this step, CS generates the random number r1 and computes R1=r1.P using ECC point multiplication. Moreover, it calculates the time stamp Tcs and parameters M1=(R1||PIDcs||Tcs) and sent to EV.

Step 2: On the receiving M1, EV extracts R1, PIDcs, and Tcs and checks if Tcs is within the permissible limit. Now EV calculates R2=Skev.R1 using received R1. Further it calculates $Auth_{EV-CS}$= h(R1||R2||PIDev||PIDcs||Tev) and $Auth_{EV-SP}$= h(R1||R2||PIDev||PIDsp||Tev) and it sends $Auth_{EV-CS}$, $Auth_{EV-SP}$,Tev,PIDev towards CS.

Step 3: CS extracts R1, IDcs,Tcs and calculates R2=SKev.R1. Now CS computes $Auth_{EVCS}$*= h(R1||r1.PKev||PIDev||PIDcs||Tev). If $Auth_{EVCS}$* equals $Auth_{EVCS}$, it authenticates or tears down the connection. Further it calculates $Auth_{CS-SP}$= h(R3||PIDcs||PIDsp||Tcs||$Auth_{EVCS}$). Now CS send $Auth_{CS-SP}$,Tev,r1,r2,R2,PIDev,PIDcs toward eMSP.

Step 4: EV sends $Auth_{CS-SP}$,Tcs,Tev,r1,r2,R2,PIDev,PIDcs toward e-MSP. Now e-MSP calculates $Auth_{CS-SP}$= h(r2.PKcs||PIDcs||PIDsp||Tcs||$Auth_{EVCS}$*). Check if $Auth_{CS-SP}$* is equal to $Auth_{ECS-SP}$, then CS authenticates else, it tears down the connection. Now computes $Auth_{SP}$= h(R5||PIDcs||PIDev||Tcs||PIDsp||Tsp) and sends toward CS.

Step 5: CS calculates $Auth_{SP}$*= h(r1.PKsp||PIDcs||PIDev||Tcs||PIDsp||Tsp). Check if $Auth_{SP}$* is equal to $Auth_{SP}$ the SP authenticate else to tear down the connection. Further CS transmits $Auth_{SP}$,r1,Tsp.

Step 6: After receiving $Auth_{SP}$ EV calculates $Auth_{SP}$*=h(r1.PKsp||PIDcs||PIDev||Tcs||PIDsp||Tsp).Check if $Auth_{SP}$* is equal to $Auth_{SP}$ the SP authenticate else tear down connection.

3.2.4. Consensus mechanism and energy trading

The PBFT consensus mechanism is commonly employed in consortium blockchains due to its superior efficiency compared to the PoW and PoS consensus algorithms utilized in public blockchains. PBFT is preferred as it requires less computation and energy. Moreover, since the PBFT algorithm can also be utilized in consortium blockchains, our scheme selects the voting-based PBFT algorithm.

After the charge or discharge, the EV updates the energy trading transaction details to the corresponding CS. The PBFT consensus mechanism is used for updating the global ledger. It is considered that CSs are equipped with sufficient resources and can write a block in the distributed global ledger.

Step 1: After completion of MA between EV and CS, EV sends the transaction details to the CS, which is further transferred to SP. e-MSP broadcasts the energy transaction details to all connected CSs on the blockchain network. Before transferring them to the blockchain global ledger, the energy transaction details are stored in their respective memories.

Step 2: Amongst the registered CSs, one is selected as the "Leader" node and the rest as the "slave" node. The main responsibility of the "Leader" is to maintain the consensus among Nodes and avoid the voting process. The leader selection among the available CSs is based on the Leader selection algorithm. The steps of the Leader selection algorithm are as follows:

i) Each node CS has some votes, say V_m (where V_m is the number of EV registered to the concerned node)

ii) Voting process starts (i=0 to i= Max number of nodes)

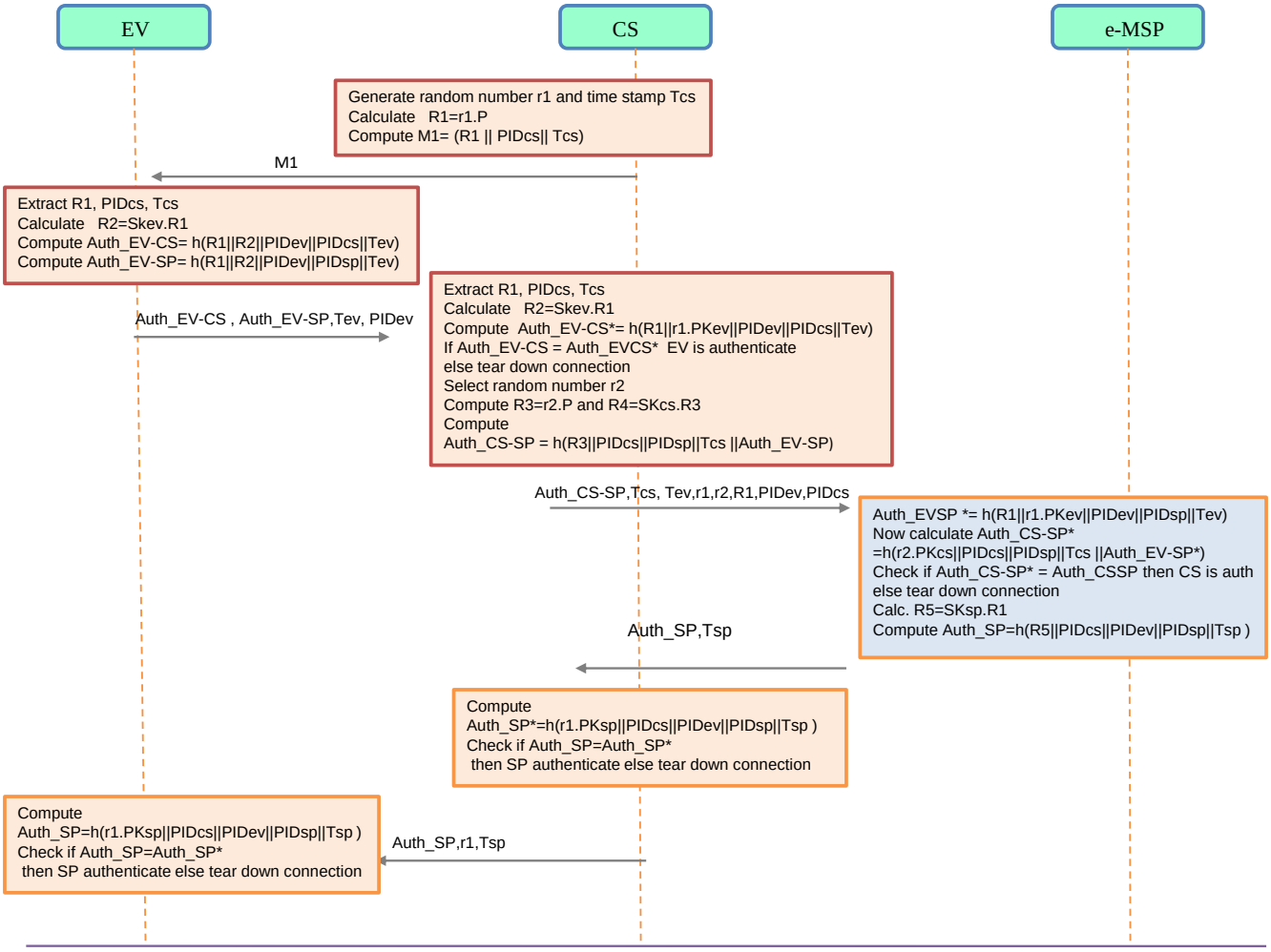

Figure 2: Mutual authentication phase

iii) Each node casts votes to Nodes it trusts most (Except itself)
iv) Node which gets maximum votes Vm, selected as Leader Node
v) This process is repeated after the writing of each block.
Step 3: After a successful energy transaction between EV-CS, the CS transmits the transaction detail to the e-MSP. Further, e-MSP transmits detailed information to all the CSs available on the blockchain. Further, the CS saves the transaction details in the respective cache before relaying them to the blockchain.
Step 4: Blocks with transaction details are created after a fixed time interval. After that, the voting process is completed by the leader node. Initially, the leader requested slave nodes to post their votes.
Step 5: After it, the slave nodes post their votes. According to the received votes from slave nodes, the leader node makes a consensus to publish the generated block having the energy trading details on the global ledger of the blockchain.

4. Results and Discussions

4.1. Security analysis of proposed sTrade

In this subsection, the robustness of the proposed sTrade against the following attack is assessed.
1) Replay Attack:
In this type of attack, the intruder sends repeated messages. sTrade ensures that each message is computed with newly generated timestamps and random nonce. Upon reaching the receiver, these timestamps and nonce are verified to prevent replay attacks by malicious adversaries. Since the time difference (ΔT) between timestamps is typically small, any attempt by an intruder A to replay previous messages can be easily identified by the message-receiving entity. As a result, sTrade effectively thwarts replay attacks from passive adversaries.
2) Man-in-the-Middle (MiTM) :
Suppose intruder A intercepts messages M1, M2, and M3 from the public channels to launch a man-in-the-middle attack. But $Auth_{EV-CS}$ and $Auth_{EV-SP}$ can not be computed without R2, which is calculated using secret key SK. Similarly, $Auth_{CS-SP}$ is calculated using R3 and R4, which are computed using a secret key and random number. Hence adversary can not launch

MiTM attack.

3) Anonymity Preservation:

In the proposed sTrade, the secret credentials such as secret keys and pseudo identities, are not transmitted in plaintext format. Random numbers (r1 and r2) and time stamps (Tev and Tcs) are generated during the message exchanges. The authentication messages AuthCS and AuthEV get fresh values in each session. So the proposed scheme supports the anonymity between EVs and CSs.

4) Ephemeral Secret Leakage Attack :

The significance of this attack lies in its ability to gauge the effectiveness of a security scheme in safeguarding the session key. If the session key is generated through long-term and short-term secrets, it can thwart a session key leakage attack. In this model, an adversary denoted as A, can pilfer session states and secret values. In the proposed sTrade system, the computed session keys (SKev and SKcs) leverage long-term secrets (identities and secret keys) as well as short-term secrets (random nonce) from different parties, which are unknown to A. Without knowledge of the long-term secrets, it would be impractical for A to deduce the session key solely through session hijacking attacks involving only short-term secrets.

5) Integrity Preservation:

While EV communicates with CS, EV and CS carry their own generated session keys. EV and CS generate random numbers r1 and r2 in each session. The randomly generated new EV keys guarantee the confidentiality and integrity of the message transmission.

6) Denial of Service (DoS) Attack:

In this attack, adversary A aimed to disrupt or disable the availability of a computer system or network. These attacks are typically carried out by flooding the target system or network with an overwhelming amount of malicious requests or data, causing the system to become unresponsive or crash. In sTrade, each message contains a time stamp, and if the received message time difference is greater than the threshold limit (Δt) , the message is discarded. Hence our scheme prevents Dos attack.

4.2. Performance evaluation and comparisons

sTrade have formally evaluated the scheme's security with the AVISPA simulation tool. The performance of proposed scheme is compared with related protocol like [32], [15] , [33] and [17] in terms of computational and communicational overhead.

Table 3: Execution time of cryptographic operation (ms)

Primitive	EV side	CS side
T_h	0.309	0.055
T_{mtp}	0.385	0.114
T_{senc}	0.018	0.003
T_{sdec}	0.014	0.003
T_{ecm}	2.288	0.674
T_{eca}	0.016	0.002
T_{bp}	32.084	4.716
T_{mul}	0.011	0.002
T_{add}	0.010	0.001
T_{exp}	0.228	0.039

4.2.1. Security verification using AVISPA tool

This subsubsection formally verifies our security protocol using the widespread AVISPA simulation tool. The role of each entity is defined using the HLPSL programming language. It uses two popular backends for the program's execution, i.e., OFMC and Cl-AtSe. The results show that our protocol is safe. The security of the protocol is verified on both backends. AVISPA shows different security attacks during the protocol simulation in the intruder section[34] if the protocol is unsafe. This protocol uses the Dolev–Yao model as the intruder model.

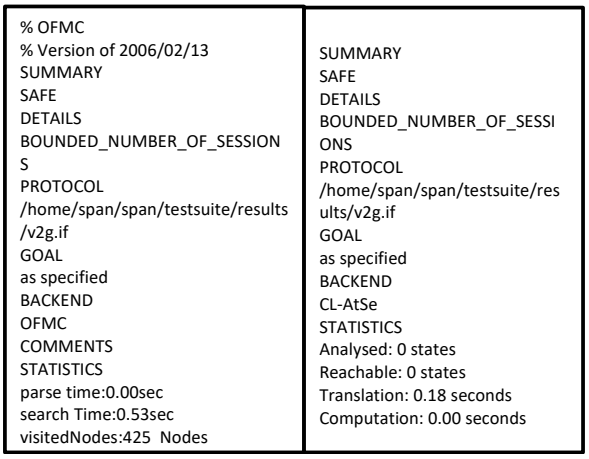

Figure 3: AVISPA OFMC and CL-Atse

4.2.2. Communication overhead comparison

In this subsubsection, sTrade has compared the communicational cost of the proposed blockchain-based V2G scheme with other popular schemes, namely [32], [15], [33], and [17].

Table 4: Communication cost comparison with related prior works

Scheme	No of messages	Total cost (bits)
Farooq, et al. 2020 [32]	6	4032
Wang et, al. 2021 [15]	1	2658
Iqbal et, al. 2021 [33]	4	3210
Wazid, et al. 2022 [17]	3	2208
Our scheme(sTrade)	5	1750

The comparison was based on several factors, including the size of the one-way hash function (256 bits), various identities (160 bits), random nonce (160 bits), and ECC point multiplication (320 bits) used in the schemes.The communication cost of [32], [15], [33] and [17] is estimated as 4032 bits, 2658 bits,3210 bits, 2208 bits respectively while the communication cost of our proposed protocol is 1710 bits. Table 4 show that our scheme requires less overhead compared to other existing schemes.

Table 5: Cryptographic operation and total computational cost comparison

Scheme	EV/SM side	CS/UC side	Total Time (ms)
Farooq, et al. 2020 [32]	$3T_{ecm} + T_h + T_{bp} + T_{mul}$	$T_h + T_{mtp} + 6T_{ecm} + 2T_{bp} + T_{mul}$	53.029
Wang, et al. 2021 [15]	$4T_{ecm} + 2T_h + T_{add}$	$6T_{ecm} + 2T_h + T_{add}$	13.935
Iqbal, et al. 2021 [33]	$T_{exp} + 2T_h + 2T_{ecm}$	$2_{Texp} + 4T_h + 4T_{ecm}$	8.416
Wazid, et al. 2022 [17]	$2T_{ecm} + 2T_h + T_{add}$	$4T_{ecm} + 4T_h + 2T_{add}$	17.667
Our scheme(sTrade)	$2T_{ecm} + 3T_h + T_{add}$	$2T_{ecm} + 3T_h + T_{add}$	7.027

4.2.3. Computational overhead analysis

In this subsubsection, our proposed scheme has compared the computational overhead of the proposed blockchain-based V2G scheme with other popular schemes [32], [15], [33] and [17]. The overhead costs involved in the registration phase are very low and hence not considered in the calculation, while computation costs involved in MA of EV and CS are considered. To compare the computational time of different schemes, the time taken for different cryptography operations in MIRACL crypto library [35] is considered. Execution time was calculated using Ubuntu 20.04 LTS, 1.4 GHz Quad-core processor, cores 4, 64-bit OS, 1 GB RAM [35]. Different cryptography operations execution time is shown in Table 3. Let T_h execution time required for hash function,T_{bp} bi-linear pairing,T_{senc} ecc encryption,T_{mtp} map to point,T_{eca} ecc addition, multiplication, T_{sdec} ecc decryption, T_{ecm} multiplication, T_{add} modular addition, T_{mul} modular multiplication, T_{exp} modular exponential respectively.
The execution time of different schemes are shown in Table 5. The computational overhead of scheme [32],[15],[33] and [17] are 53.029 ms, 13.935 ms, 8.416 ms, 17.667 ms respectively while our proposed scheme overhead is 7.027 ms. Table 5 shows that our proposed model requires less computational overhead compared to other popular schemes.

4.3. Discussion

This subsection presents the challenges of blockchain and the advantages and limitations of blockchain adoption in V2G energy trading.

4.3.1. Challenges of V2G energy trading network:

The high mobility and dynamic movement of EVs in the network pose challenges in accurately analyzing the exact count at any moment. The utilization of various communication technologies for V2G communication significantly impacts the network's complexity. Reliable and low-latency communication services are essential for meeting the requirements of modern applications. With the emergence of smaller, variable, and less predictable renewable energy sources in recent years, an effective DRM has become crucial for V2G energy trading. Furthermore, V2G systems may be vulnerable to machine learning attacks, where malicious EVs impersonate multiple non-existent EVs to manipulate the system.

4.3.2. Blockchain-based V2G energy trading network contribution and advantages

The application of blockchain in the proposed sTrade provides several benefits. As V2G energy trading grows, effective communication between EVs and CS becomes crucial. With its decentralized and transparent nature, blockchain eliminates the need for centralized entities, making it a promising option for transparent energy trading in the proposed V2G system. Integrating blockchain technology into V2G systems enhances security and reliability by addressing risks associated with interruptions and single points of failure. Blockchain's decentralized approach ensures seamless energy trading even if nodes fail, enhancing the resilience of the V2G system. Using cryptographic techniques and consensus mechanisms in sTrade ensures data immutability, enhancing the security of V2G energy trading services. This creates a robust system where energy transactions cannot be easily altered or deleted, adding a layer of security to the V2G network. Public blockchains are open and accessible to all entities, providing transparency to the V2G network. This allows full access to the data stored in the blockchain but requires careful consideration of data privacy and security.

4.3.3. Limitations of Blockchain based V2G system

Our scheme has proposed a blockchain-based V2G energy trading network. Although much work has been conducted, blockchain is still experiencing some limitations and potential restrictions related to its integration in the real world. The current regulatory system for V2G trading cannot facilitate energy trading from prosumers to consumers and does not actively promote the integration of blockchain and smart contracts into the V2G network. Integrating blockchain into V2G smart grids poses challenges in handling large data and transactions in a dynamic environment with moving EVs. This limitation of blockchain technology hinders its immediate integration with the V2G network, considering the fast-paced nature of EV movements and energy transactions in V2G systems. Entities in the V2G network, such as sensors, RSUs, EV batteries, and CS, often have limited resources, including processing power, storage space, battery capacity, and network connectivity, which can impact the network's performance and efficiency. The proposed sTrade PBFT blockchain for V2G security provides data immutability, but it may not guarantee immediate security and privacy due to its reliance on other techniques and factors. Ad-

ditional measures may be needed to enhance security and privacy in V2G systems.

5. Conclusion

This paper proposes V2G energy trading based on blockchain technology for smart transportation. Blockchain-based energy trading performs by removing centralized third-party systems. Therefore, the consensus mechanism and mutual authentication between distributed EVs and CS is crucial. This scheme proposes the PBFT consensus algorithm with a scheduling feature. The proposed ECC-based hierarchical mechanism for mutual authentication in V2G systems involving EVs, CSs, and e-MSP is a novel approach promising to reduce communication and computational expenses. The results suggest its suitability for V2G scenarios, particularly for resource-constrained EVs.
In future V2V, G2V, and G2G auction-based energy trading, more applications of IoT in V2G and EVs privacy will be an extension of this research work using smart contract blockchain technology.

Acknowledgement

The authors thank SMDP-C2SD Lab, Malaviya National Institute of Technology Jaipur, and Visvesvaraya PhD. Scheme of (MEITY) Ministry of Electronics & IT, Govt. of India for supporting simulation tools to perform the experiments. The results of the research work are carried out at SMDP-C2SD Lab, MNIT Jaipur.

References

[1] A. V. Jha, B. Appasani, A. N. Ghazali, P. Pattanayak, D. S. Gurjar, E. Kabalci, D. Mohanta, Smart grid cyber-physical systems: communication technologies, standards and challenges, Wireless Networks 27 (2021) 2595–2613.

[2] R. Sharma, A. M. Joshi, C. Sahu, G. Sharma, K. T. Akindeji, S. Sharma, Semi supervised cyber attack detection system for smart grid, in: 2022 30th Southern African Universities Power Engineering Conference (SAUPEC), 2022, pp. 1–5. doi:10.1109/SAUPEC55179.2022.9730715.

[3] A. Irshad, S. A. Chaudhry, M. Alazab, A. Kanwal, M. S. Zia, Y. B. Zikria, A secure demand response management authentication scheme for smart grid, Sustainable Energy Technologies and Assessments 48 (2021) 101571.

[4] D. Puthal, S. P. Mohanty, E. Kougianos, G. Das, When do we need the blockchain?, IEEE Consumer Electronics Magazine 10 (2) (2020) 53–56.

[5] G. Sharma, A. M. Joshi, S. P. Mohanty, An efficient physically unclonable function based authentication scheme for V2G network, in: Proc. IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS), 2021, pp. 421–425.

[6] Z. Zhou, L. Tan, G. Xu, Blockchain and edge computing based vehicle-to-grid energy trading in energy internet, in: Proc. 2nd IEEE conference on energy internet and energy system integration (EI2), 2018, pp. 1–5.

[7] R. Khalid, M. W. Malik, T. A. Alghamdi, N. Javaid, A consortium blockchain based energy trading scheme for electric vehicles in smart cities, Journal of Information Security and Applications 63 (2021) 102998.

[8] R. Sharma, A. M. Joshi, C. Sahu, S. J. Nanda, Detection of false data injection in smart grid using pca based unsupervised learning, Electrical Engineering (2023) 1–14.

[9] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis, C. Douligeris, Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (ocpp), IEEE Communications Surveys & Tutorials (2022).

[10] A. Unterweger, F. Knirsch, D. Engel, D. Musikhina, A. Alyousef, H. de Meer, An analysis of privacy preservation in electric vehicle charging, Energy Informatics 5 (1) (2022) 1–27.

[11] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things, IEEE Transactions on Industrial Informatics 14 (8) (2017) 3690–3700.

[12] D. Puthal, S. P. Mohanty, Proof of authentication: IoT-friendly blockchains, IEEE Potentials 38 (1) (2019) 26–29. doi:10.1109/MPOT.2018.2850541.

[13] P. Gope, B. Sikdar, An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication, IEEE Transactions on Smart Grid 10 (6) (2019) 6607–6618.

[14] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, D. N. K. Jayakody, A blockchain-based framework for lightweight data sharing and energy trading in V2G network, IEEE Transactions on Vehicular Technology 69 (6) (2020) 5799–5812.

[15] W. Wang, H. Huang, L. Zhang, C. Su, Secure and efficient mutual authentication protocol for smart grid under blockchain, Peer-to-Peer Networking and Applications 14 (5) (2021) 2681–2693.

[16] A. Kumari, M. Trivedi, S. Tanwar, G. Sharma, R. Sharma, SV2G-ET: A secure vehicle-to-grid energy trading scheme using deep reinforcement learning, International Transactions on Electrical Energy Systems 2022 (2022).

[17] M. Wazid, B. Bera, A. K. Das, S. P. Mohanty, M. Jo, Fortifying smart transportation security through public blockchain, IEEE Internet of Things Journal 9 (17) (2022) 16532–16545.

[18] Y. Wang, L. Yuan, W. Jiao, Y. Qiang, J. Zhao, Q. Yang, K. Li, A fast and secured vehicle-to-vehicle energy trading based on blockchain consensus in the internet of electric vehicles, IEEE Transactions on Vehicular Technology (2023).

[19] S. Aggarwal, N. Kumar, A consortium blockchain-based energy trading for demand response management in vehicle-to-grid, IEEE Transactions on Vehicular Technology 70 (9) (2021) 9480–9494.

[20] F. Knirsch, A. Unterweger, D. Engel, Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions, Computer Science-Research and Development 33 (1) (2018) 71–79.

[21] L. Qi, X. Li, B. Qi, H. Wang, Shared economy model of charging pile based on block chain ecosystem, Electric Power Construction 38 (9) (2017) 1–7.

[22] V. Odelu, A. K. Das, M. Wazid, M. Conti, Provably secure authenticated key agreement scheme for smart grid, IEEE Transactions on Smart Grid 9 (3) (2016) 1900–1910.

[23] A. Abdallah, X. Shen, A. Abdallah, X. Shen, Smart grid security security and privacy of customer-side networks, Security and Privacy in Smart Grid (2018) 27–64.

[24] H. Liu, Y. Zhang, S. Zheng, Y. Li, Electric vehicle power trading mechanism based on blockchain and smart contract in V2G network, IEEE Access 7 (2019) 160546–160558.

[25] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, J. J. Rodrigues, An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment, in: Proc. IEEE International Conference on Communications Workshops (ICC Workshops), 2019, pp. 1–6.

[26] S. Aggarwal, N. Kumar, P. Gope, An efficient blockchain-based authentication scheme for energy-trading in V2G networks, IEEE Transactions on Industrial Informatics 17 (10) (2021) 6971–6980. doi:10.1109/TII.2020.3030949.

[27] A. Jain, A. M. Joshi, Device authentication in IoT using reconfigurable PUF, in: Proc. 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), 2019, pp. 1–4.

[28] X. Huang, C. Xu, P. Wang, H. Liu, Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem, IEEE Access 6 (2018) 13565–13574. doi:10.1109/ACCESS.2018.2812176.

[29] S. P. Mohanty, V. P. Yanambaka, E. Kougianos, D. Puthal, PUF chain: A hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (IoE), IEEE Consumer Electronics Magazine 9 (2) (2020) 8–16.

[30] R. Basmadjian, B. Kirpes, J. Mrkos, M. Cuchỳ, A reference architecture for interoperable reservation systems in electric vehicle charging, Smart Cities 3 (4) (2020) 1405–1427.
[31] M. Kim, J. Lee, J. Oh, K. Park, Y. Park, K. Park, Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers, Applied Energy 322 (2022) 119445.
[32] S. M. Farooq, S. S. Hussain, T. S. Ustun, A. Iqbal, Using id-based authentication and key agreement mechanism for securing communication in advanced metering infrastructure, IEEE Access 8 (2020) 210503–210512.
[33] A. Iqbal, A. S. Rajasekaran, G. S. Nikhil, M. Azees, A secure and decentralized blockchain based EV energy trading model using smart contract in V2G network, IEEE Access 9 (2021) 75761–75777.
[34] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, et al., The AVISPA tool for the automated validation of internet security protocols and applications, in: Proc. International conference on computer aided verification, Springer, 2005, pp. 281–285.
[35] "MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library", Accessed on October 2020. [online]. Available: https://github.com/miracl/MIRACL.