sensors

MDPI

Article

A Secure Charging System for Electric Vehicles Based on Blockchain

MyeongHyun Kim [1], KiSung Park [1,*], SungJin Yu [1], JoonYoung Lee [1], YoungHo Park [1,*], Sang-Woo Lee [2] and BoHeung Chung [2]

[1] School of Electronics Engineering, Kyungpook National University, Daegu 41566, Korea
[2] Information Security Research Division, Electronics and Telecommunications Research Institute, Daejeon 34129, Korea
* Correspondence: kisung2@ee.knu.ac.kr (K.P.); parkyh@knu.ac.kr (Y.P.); Tel.: +82-53-950-7842 (Y.P.)

Received: 4 June 2019; Accepted: 6 July 2019; Published: date

Abstract: Smart grids incorporating internet-of-things are emerging solutions to provide a reliable, sustainable and efficient electricity supply, and electric vehicle drivers can access efficient charging services in the smart grid. However, traditional electric vehicle charging systems are vulnerable to distributed denial of service and privileged insider attacks when the central charging server is attacked. The blockchain-based charging systems have been proposed to resolve these problems. In 2018, Huang et al. proposed the electric vehicle charging system using lightning network and smart contract. However, their system has an inefficient charging mechanism and does not guarantee security of key. We propose a secure charging system for electric vehicles based on blockchain to resolve these security flaws. Our charging system ensures the security of key, secure mutual authentication, anonymity, and perfect forward secrecy, and also provides efficient charging. We demonstrate that our proposed system provides secure mutual authentication using Burrows–Abadi–Needham logic and prevents replay and man-in-the-middle attacks using automated validation of internet security protocols and applications simulation tool. Furthermore, we compare computation and communication costs with previous schemes. Therefore, the proposed charging system efficiently applies to practical charging systems for electric vehicles.

Keywords: smart grid; internet-of-things; blockchain; electric vehicle; secure charging system

1. Introduction

With widespread adoption of electric vehicles (EVs) and internet-of-things (IoT), smart grids with IoT have become promising solutions to control distributed energy and electricity generation [1]. Internet-of-things is applicable to various forms for vehicular systems, such as vehicular ad hoc networks, vehicle to grid (V2G), vehicle to vehicle (V2V), and internet of vehicle (IoV). Vehicles generally have various communication and measuring sensors, including speed, position, Bluetooth, Wi-Fi and On-board units (OBU). The sensors in vehicle collect and share data such as speed, location, identity and movements. However, an adversary can intercept, modify and reuse the sensitive data of user, and then try to obatin user's sensitive data because it is transmitted via public network. Therefore, secure mutual authentication and key agreement must be guaranteed to provide secure communication and protect user's privacy.

In the past decades, the numerous authentication and key agreement schemes for vehicular systems in IoT have been studied to achieve essential security requirements [2–10]. Although these schemes try to ensure privacy and enhance efficiency, their scheme is vulnerable to various potential attacks such as distributed denial of service and privileged insider attacks because it is based on trusted third party to provide high security level. If the trusted third party is compromised, their schemes cannot provide services. For these reasons, authenticaion and key agreement schemes without a trusted third party must be proposed to achieve integrity, confidentiality, availability and reliability, considering resource-constrained devices

The smart grid provides reliable, sustainable, stable, and efficient electricity supply. EV charging management is a particularly important issue for smart grids, and related studies have been proposed [11–16], providing EV charging for users when they want to use it. However, traditional smart grid systems provide charging services based on a third party and are vulnerable to various attacks, including distributed denial of service and privileged insider attacks. If the third party is compromised, users cannot use EV charging, and smart grid systems with IoT must also consider efficiency, because EV sensors as OBU in EV also have low power and small memory.

Several studies have proposed blockchain approaches to overcome these security weaknesses and enhance efficiency [17–22]. Blockchain [17] technology guarantees decentralization, verification, and integrity, and is applicable to various fields, including smart grids, healthcare, finance, markets, and voting. Generally, blockchains consists of data blocks, called transactions, where each transaction includes data regarding previous transactions using a hash algorithm [18]. However, early blockchain studies focused on cryptocurrency, e.g., Bitcoin and Ethereum, which have significant scalability problems. Hyperledgers [19], which do not generate cryptocurrency, have been proposed to overcome these problems and solve scalability. Huang et al. [20] proposed blockchain based EV charging management security model using smart contracts and the lightning network.

This paper demonstrates that Huang et al.'s charging system [20] has inefficient charging mechanisms such as the deposit problem, generating transaction and cost of transaction fee. Huang et al.'s system also does not guarantee security of keys. Consequently, we propose a secure charging system for electric vehicles using a hyperledger to improve security and efficiency. Our main contributions are as follows.

(1) We demonstrate security weaknesses of Huang et al.'s model, and highlight its inefficiencies.
(2) We propose a secure charging system for EV based on blockchain to solve these security weaknesses and improve efficiency.
(3) We perform informal analysis to demonstrate the proposed system is secure against various attacks, and prove that it provides secure mutual authentication using Burrows–Abadi–Needham (BAN) logic. We also perform formal security verification using the AVISPA tool and compare performances with previous schemes.
(4) We analyze the computational and communication costs compared with other related existing schemes.

1.1. Organization

The remainder of this paper is organized as follows. Section 2 introduces the proposed blockchain-based EV charging model. Sections 3 and 4 review Huang et al.'s scheme and analyze its security flaws. Section 5 proposes a secure charging system for EV based on blockchain. Section 6 provides informal analysis to verify the proposed system's security and proves that the system mutual authentication using BAN logic. We also demonstrate that the proposed system is secure against replay and man-in-the-middle attacks using the AVISPA simulation tool. Section 7 compares the proposed system's performance with related previous schemes. Finally, Section 8 summarizes and concludes the paper.

1.2. Related Works

There are several authentication and key agreement schemes for wireless sensor networks to resolve privacy and security issues [23–26]. In 2011, Roman et al. [23] analyzed existing authentication and key management schemes for WSN in IoT to enhance security and performance. In 2014, Turkanovic et al. [24] first proposed an authentication and key agreement scheme based on IoT considering resource-constrained devices. However, in 2016, Amin et al. [25] showed that Turkanovic et al.'s scheme was vulnerable to smart card theft, offline identity-password guessing and user impersonation attacks, and proposed an enhanced authentication scheme to overcome these security problems. However, Lu [26] et al. pointed out that Amin et al.'s scheme did not prevent known session-specific temporary information attack and proposed improved authentication and key agreement scheme using symmetric key.

Numerous privacy protection schemes for a vehicular system in IoT ensure security and improve efficiency [2–10]. In 2016, Lo and Tasi [2] proposed an efficient authentication scheme for vehicular sensor networks to improve performance. Kumari et al. [3] also proposed a secure trust-extended authentication scheme for vehicular ad-hoc networks to ensure authenticity of messages. In 2017, Chin et al. [4] discussed the security vulnerabilities in the internet-of-things-based smart grid and Liu et al. [5] proposed efficient dual authentication and key agreement scheme in IoV. Mohit et al. [6] also proposed authentication protocol for smart vehicular system in IoT considering energy efficiency of sensor and Guo et al. [7] proposed secure information collection scheme for big data in large scale IoV. Zhou et al. [8] proposed an enhanced privacy-preserving authentication scheme for vehicle sensor network to overcome security weaknesses of the Kumari et al.'s scheme [3]. In 2018, Shen et al. [9] proposed privacy-preserving and lightweight key agreement scheme for V2G in social IoT to guarantee security of smart grid. In 2019, Wu et al. [10] proposed mutual authentication scheme for V2V in vehicular ad hoc network to achieve better performance and security.

Several previous studies have considered EV charging systems [11–16]. In 2013, Gan et al. [11] proposed a decentralized protocol for EV charging to improve charging efficiency. In 2016, Xu et al. [12] proposed dynamic EV scheduling using less laxity and longer remaining processing time principle. In 2010 and 2012, Lu et al. [13] and Kim et al. [14] proposed scheduling mechanisms to reduce waiting times at charging stations. In 2016, Tian et al. [15] proposed recommendation system in real-time to provide charging station information. Tang and Zhang [16] proposed a low complexity EV charging scheduling algorithm using near optimal solutions.

Many studies have guaranteed decentralization, verification, and integrity [17,19,21,22,27]. However, initial blockchain models have scalability problems. Lightning network [21] and hyperledger [19] networks have been proposed to overcome this problem and improve efficiency. Lightning networks establish trading channels outside the main blockchain to enhance network performance. Hyperledger solves scalability problem and removes the requirement for cryptocurrency transactions to enhance the performances. These systems incorporate smart contracts, a set of commitments, that improve performance and privacy without requiring a trusted third party [22,27].

Several blockchain-based EV charging management systems have been proposed to improve performance [20,28–30]. In 2017, Dubois et al. [28] proposed an app-based blockchain system using smart contracts to provide a charging service between EVs and charging stations without requiring a trusted third party. Knirsch et al. [29] proposed an EV charging system where the EV finds the best charging station by bidding on the blockchain. Li et al. [30] proposed a consortium blockchain for energy trading in the industrial IoT to guarantee fast and reliable energy trading using the Stackelberg game. In 2018, Huang et al. [20] proposed a blockchain-based EV charging management security model, incorporating authentication mechanisms using smart contracts and the lightning network. However, the lightning network has an inefficient charging mechanism and Huang et al.'s system does not guarantee security of keys.

2. System Model

This section presents a secure charging system model for EV based on blockchain and basic concept of hyperledger.

2.1. Hyperledger

Hyperledger [19] is an open source project proposed by the Linux Foundation in 2015. The purpose is to promote cross-industry cooperation with blockchain technology. Hyperledger focuses on enhancing blockchain performance and reliability without requiring cryptocurrency.

Hyperledger architecture comprises nine blockchain components.

1. Consensus layer: ensures agreement between transaction order and checks their validation.
2. Smart contract layer: processes transaction requests and verifies smart contracts are valid.
3. Communication layer: guarantees security for messages transmitted between nodes.
4. Data store abstraction: manages data.
5. Crypto abstraction: includes cryptographic algorithms or modules.
6. Identity service: sets up the blockchain network, manages user and system node registration, and provides authentication and authorization.
7. Policy services: provide various policies for blockchain systems.
8. APIs: provide various blockchain interfaces.
9. Interoperation: allows interoperation among blockchain instances.

Hyperledger provides scalability, confidentiality, complexity, essential security requirements, and compliance; and can also provide distributed ledgers, smart contracts, and friendly interfaces. Therefore, hyperledgers can be applied to various fields and disseminate blockchain technologies for cross-industry applications.

2.2. System Model

Figure 1 presents the proposed charging system for EV based on blockchain and our charging system comprises three entities: operator, energy aggregator (EAG), and user/EV; and incorporates four phases: initialization, registration, authentication, and charging, as follows.

1. EV registers their identity with the operator to access charging services.
2. EV and EAG authenticate each other.
3. EAG generates transactions.
4. EAG verifies the transaction is valid and records transactions on blockchain networks.

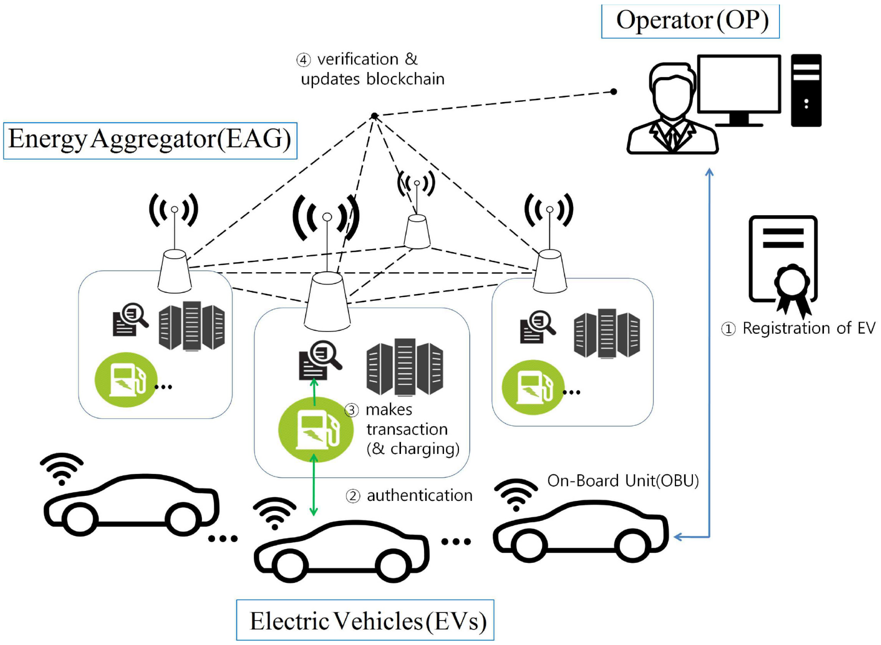


Figure 1. Proposed blockchain based charging system model for electric vehicle.

3. Review of Huang et al.'s Scheme

This section reviews Huang et al.'s blockchain based EV charging system [20], comprising four phases: registration, scheduling, authentication, and charging.

3.1. Registration Phase

Figure 2 shows how Huang scheme charging management includes EVs, charging piles (CPs) and operators (OP). Each participant is required to register in the open blockchain system. In Huang et al.'s scheme, lightning network transaction management system adopts an internet based cloud platform. The detailed steps are as follows.

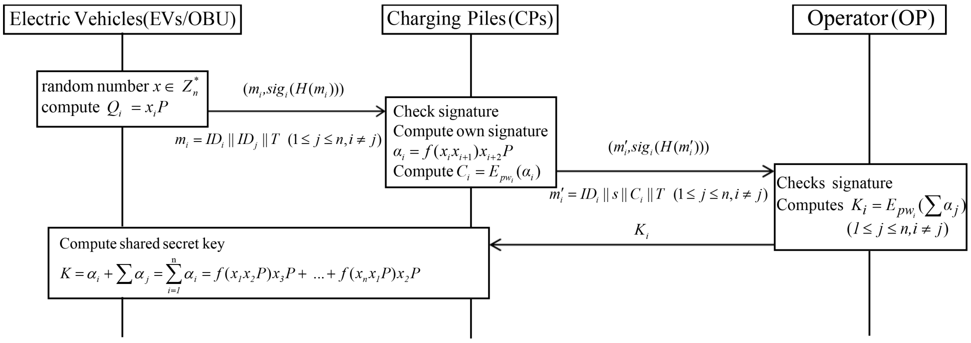

Electric Vehicles(EVs/OBU)
Charging Piles(CPs)
Operator(OP)
random number $x \in Z_n^*$
compute $Q_i = x_i P$
$(m_i, sig_i(H(m_i)))$
$m_i = ID_i \| ID_j \| T \ (1 \le j \le n, i \ne j)$
Check signature
Compute own signature
$\alpha_i = f(x_i x_{i+1}) x_{i+2} P$
Compute $C_i = E_{pw_i}(\alpha_i)$
$(m_i', sig_i(H(m_i')))$
$m_i' = ID_i \| s \| C_i \| T \ (1 \le j \le n, i \ne j)$
Checks signature
Computes $K_i = E_{pw_i}(\sum \alpha_j)$
$(1 \le j \le n, i \ne j)$
K_i
Compute shared secret key
$K = \alpha_i + \sum \alpha_j = \sum_{i=1}^{n} \alpha_i = f(x_1 x_2 P) x_3 P + \ldots + f(x_n x_1 P) x_2 P$

Figure 2. Registration phase of Huang et al.'s scheme.

Step 1: EVs $\{V_1, V_2, \cdots, V_n\}$ choose a random number $x \in Z_n^*$ and calculate $Q_i = x_i P$. The EVs request a registration in a blockchain and broadcast $m_i = ID_i || ID_j || T, (1 \le j \le n, i \ne j)$, and $(m_i, sig_i(H(m_i)))$.

Step 2: CPs check whether the received signature is valid, and then compute signature $\alpha_i = f(x_i x_{i+1}) x_{i+2} P$ and $C_i = E_{pw_i}(\alpha_i)$. Then, CPs send $m_i = ID_i || s || C_i || T$ and $(m_i', sig_i(H(m_i')))$ to the OP in the blockchain.

Step 3: OP verifies the received the signature is valid and reuses PW_i, where PW_i is shared with each participant to decrypt α_i. Subsequently OP computes $K_i = E_{PW_i}(\sum \alpha_j)(1 \le j \le n, i \ne j)$ and broadcasts it in the blockchain.

Step 4: After receiving key K_i from the OP, each participant decrypts K_i and computes session key $K = \alpha_i + \sum \alpha_j = \sum_{i=1}^{n} \alpha_i = f(x_1 x_2 P) x_3 P + \cdots + f(x_n x_1 P) x_2 P$. When a request is recorded in the blockchain, it is checked by all CPs.

3.2. Scheduling Phase

Figure 3 shows the Huang scheme includes four scheduling strategies to provide charging services and improve charging efficiency: minimum time, minimum waiting time, minimum total cost, and shortest path.

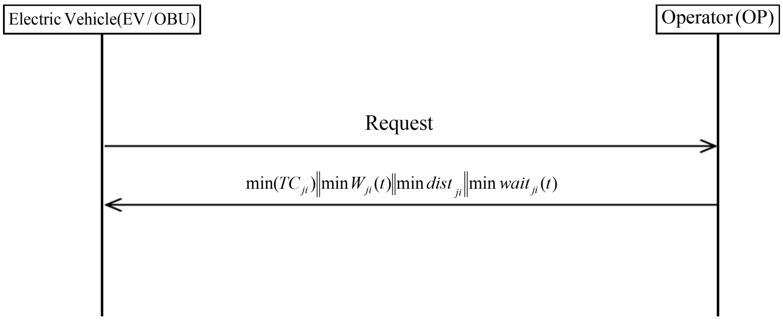

Electric Vehicle(EV/OBU)
Operator(OP)
Request
$\min(TC_{ji}) \| \min W_{ji}(t) \| \min dist_{ji} \| \min wait_{ji}(t)$

Figure 3. Scheduling phase of Huang et al.'s scheme.

3.3. Authentication Phase

Figure 4 shows that EV and CP perform point-to-point (P2P) transactions under the Huang scheme, followed with mutual authentication to improve trading flexibility. Depending on scheduling strategies, the EV receives the recommendation from the OP, then EV and the selected CP authenticate each other, with mutual authentication performed between EV and CP when the EV arrives at the CP. The detailed authentication steps are as follows.

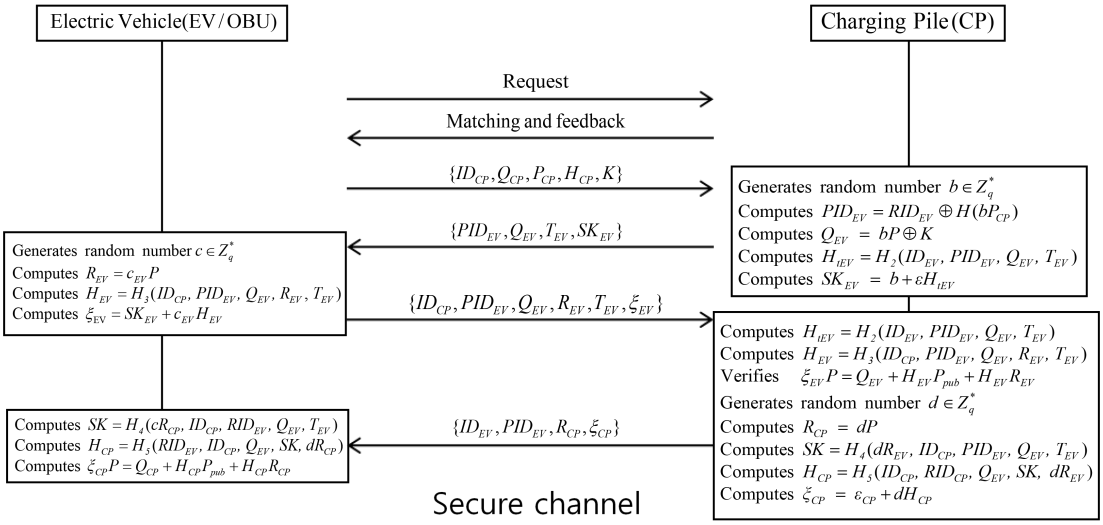

Electric Vehicle(EV/OBU)
Charging Pile(CP)
Request
Matching and feedback
$\{ID_{CP}, Q_{CP}, P_{CP}, H_{CP}, K\}$
Generates random number $b \in Z_q^*$
Computes $PID_{EV} = RID_{EV} \oplus H(bP_{CP})$
Computes $Q_{EV} = bP \oplus K$
Computes $H_{tEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$
Computes $SK_{EV} = b + \varepsilon H_{tEV}$
$\{PID_{EV}, Q_{EV}, T_{EV}, SK_{EV}\}$
Generates random number $c \in Z_q^*$
Computes $R_{EV} = c_{EV}P$
Computes $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$
Computes $\xi_{\mathrm{EV}} = SK_{EV} + c_{EV}H_{EV}$
$\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$
Computes $H_{tEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$
Computes $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$
Verifies $\xi_{EV}P = Q_{EV} + H_{EV}P_{pub} + H_{EV}R_{EV}$
Generates random number $d \in Z_q^*$
Computes $R_{CP} = dP$
Computes $SK = H_4(dR_{EV}, ID_{CP}, PID_{EV}, Q_{EV}, T_{EV})$
Computes $H_{CP} = H_5(ID_{CP}, RID_{CP}, Q_{EV}, SK, dR_{EV})$
Computes $\xi_{CP} = \varepsilon_{CP} + dH_{CP}$
$\{ID_{EV}, PID_{EV}, R_{CP}, \xi_{CP}\}$
Computes $SK = H_4(cR_{CP}, ID_{CP}, RID_{EV}, Q_{EV}, T_{EV})$
Computes $H_{CP} = H_5(RID_{EV}, ID_{CP}, Q_{EV}, SK, dR_{CP})$
Computes $\xi_{CP}P = Q_{CP} + H_{CP}P_{pub} + H_{CP}R_{CP}$
Secure channel

Figure 4. Authentication phase of Huang et al.'s scheme.

Step 1: EV sends identity ID_{EV} to the CP, and then the CP checks whether it is valid through the blockchain networks. If it is valid, the CP returns charging request to the EV.

Step 2: After receiving the charging request from the CP, the EV sends $\{Q_{CP}, P_{CP}, ID_{CP}, H_{CP}, K\}$ to the CP.

Step 3: CP selects a random number $b \in Z_q^*$, current timestamp T_i, and calculates $PID_{EV} = RID_{EV} \oplus H_1(bP_{CP})$, $Q_{EV} = bP \oplus K$, $H_{tEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$ and $SK_{EV} = b + \epsilon H_{tEV}$. Then, the CP sends $\{PID_{EV}, Q_{EV}, T_{EV}, SK_{EV}\}$ to the EV.

Step 4: EV selects a random number $c \in Z_q^*$, calculates R_{EV}=$c_{EV}P$, H_{EV}= $H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$ and $\xi_{EV} = SK_{EV} + c_{EV}H_{EV}$, and sends $\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$ to the CP via the secure channel.

Step 5: After receiving the message from the EV, the CP computes H_{tEV}=$H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$ and $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$, and checks the received signature. If it is not valid, the CP aborts the authentication phase. Otherwise, the CP selects a random number $d \in Z_q^*$ and computes $R_{CP} = dP$, $SK = H_4(dR_{EV}, ID_{CP}, PID_{EV}, Q_{EV}, T_{EV})$, $H_{CP} = H_5(ID_{CP}, RID_{CP}, Q_{EV}, SK, dR_{EV})$, and $\xi_{CP} = \epsilon_{CP} + dH_{CP}$. Finally, the CP sends $\{ID_{EV}, PID_{EV}, R_{CP}, \xi_{CP}\}$ to the EV.

Step 6: After receiving the message from the CP, the EV computes $SK = H_4(cR_{CP}, ID_{CP}, RID_{EV}, Q_{EV}, T_{EV})$,$H_{CP} = H_5(RID_{EV}$, and $ID_{CP}, Q_{EV}, SK, dR_{CP})$. The CP checks the received signature. If valid, the EV and CP achieve mutual authentication. Otherwise, the EV aborts mutual authentication. After mutual authentication, the session key SK is used to encrypt messages to ensure secure communications.

3.4. Charging Phase

Figure 5 shows the Huang scheme charging phase. After completing authentication, the EV performs charging and updates the transactions. The commitment is recorded in the blockchain. The detailed steps are as follows.

Step 1: EV calculates commitment $C = H_5(ID_{EV}, R_{CP}, \xi_{CP}P)$ including EV's identity, random parameter, and signature.

Step 2: CP verifies whether commitment $C = H_5(ID_{EV}, R_{CP}\xi_{CP}P)$ and current time stamps are valid. If valid, the CP starts charging for EV. Otherwise, this phase is aborted.

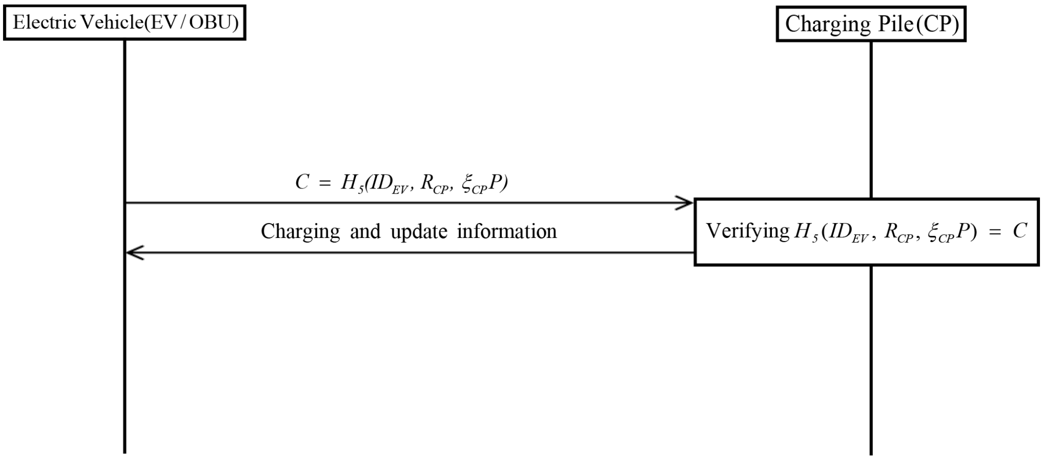

Electric Vehicle(EV/OBU)
Charging Pile(CP)
$C = H_5(ID_{EV}, R_{CP}, \xi_{CP}P)$
Charging and update information
Verifying $H_5(ID_{EV}, R_{CP}, \xi_{CP}P) = C$

Figure 5. Charging phase of Huang et al.'s scheme.

4. Problems of Huang et al.'s Scheme

This section discusses problems of Huang et al.'s scheme, such as deposit problem, inefficient transaction generation mechanism, and transaction cost.

4.1. Deposit Problem

In the scheduling phase of Huang et al.'s scheme, the OP recommends an efficient charging station using four strategies. However, the system has a deposit problem where EV needs to establish many payment channels for charging. In lightning networks, a deposit is used to establish a payment channel between two participants. However, an EV is mobile and cannot efficiently choose optimal charging stations because a payment channel must be established with each new charging station. Therefore, an EV unnecessarily spends many deposits, i.e., the mechanism is inefficient.

4.2. Inefficient Mechanism for Generating Transaction

The lightning network records a transaction in the blockchain when opening and closing a payment channel. When charging is completed at a charging station, the commitment transaction is generated and recorded in the blockchain. However, an EV already makes a transaction in the registration phase to allows access to the service, hence, two transactions are generated for one trade, i.e., an inefficient charging mechanism.

4.3. Cost of Transaction Fee

The Huang et al.'s scheme charges a transaction fee when a payment channel is opened or closed. However, after completing charging, an EV needs to re-register with the OP to use the service, hence re-opening the payment channel and incurring a transaction fee. Therefore, the Huang et al.'s scheme results in high transaction fees.

4.4. Security of Key

Huang et al. claimed their scheme provided known key security because the shared secret key K included unique random numbers for each participant. However, an adversary can steal the EV on-board unit (OBU) [31] and extract sensitive data stored in its memory using the power analysis attack [32,33]. Consequently, an adversary can obtain shared secret keys stored in the OBU, avoiding known key security.

5. Proposed Charging System for EV Based on Blockchain

This section proposes a blockchain based EV charging system that addresses the identified problems. Table 1 details the notation used for the proposed phases: initialization, registration, authentication, and charging.

Table 1. Notations.

Notations	Meanings
EV	Electric vehicle
EAG	Energy aggregator
OP	Operator
E_p	Elliptic curve over a finite field, where p is a large prime number
G	Base point in E_p
ID_i/PW_i	Identity/password for entity i
r_i	Private key for entity i
PK_i	Public key for entity i
a, b	Random number
k_{op}	Random number from OP
$h(\cdot)$	Hash function
$\|\|$	Concatenation operation
$\oplus$	XOR operation
SK	Session key

5.1. Initialization Phase

The operator conducts system initialization to set up the networks and EAG is registered in network. The details initialization process is as follows.

Step 1: OP selects a base point G on the elliptic curve E_p with order n, where n is a large prime number.
Step 2: EAG generates public key, private key, and random number b_1.
Step 3: OP defines network configuration including channel members and policies, records it in a blockchain, and shares it with system participants.

5.2. Registration Phase

When it wants to access the charging system, EV$_i$ generates its identity, password, public/private key pair, and then receives a random number from OP. Figure 6 shows the registration phase, with detailed steps as follows.

Step 1: EV$_i$ selects their identity ID_i, password PW_i, generates random numbers a_1 and r_{EV}, calculates a public key $r_{EV} \cdot G$ and $HID_i = h(ID_i||a_1)$, and then sends HID_i and a_1 to OP through a secure channel.
Step 2: OP chooses a random number k_{op} and calculates public key $PK_{op} = r_{op} \cdot G$, $A_i = h(HID_i||a_1)$, $B_i = A_i \oplus k_{op}$, and $C_i = h(HID_i||a_1||k_{op})$. Finally, OP sends $\{B_i, C_i\}$ to EV$_i$, modifies network configurations, and stores details in the blockchain.
Step 3: EV$_i$ computes $D_i = h(ID_i||PW_i) \oplus a_i$, $E_i = h(a_1||ID_i||PW_i) \oplus r_{EV}$; and stores $\{B_i$, C_i, D_i, and $E_i\}$ in memory.

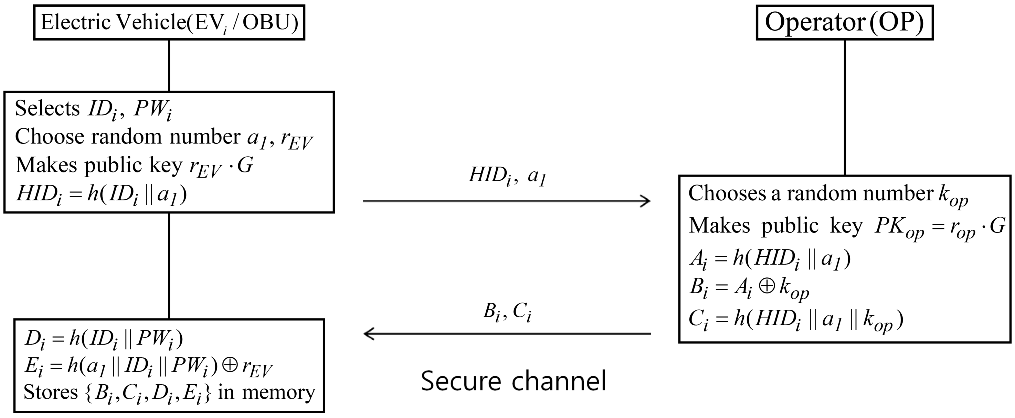

Electric Vehicle(EV$_i$ / OBU)
Operator (OP)
Selects ID_i, PW_i
Choose random number a_1, r_{EV}
Makes public key $r_{EV} \cdot G$
$HID_i = h(ID_i \| a_1)$
HID_i, a_1
Chooses a random number k_{op}
Makes public key $PK_{op} = r_{op} \cdot G$
$A_i = h(HID_i \| a_1)$
$B_i = A_i \oplus k_{op}$
$C_i = h(HID_i \| a_1 \| k_{op})$
B_i, C_i
Secure channel
$D_i = h(ID_i \| PW_i)$
$E_i = h(a_1 \| ID_i \| PW_i) \oplus r_{EV}$
Stores $\{B_i, C_i, D_i, E_i\}$ in memory

Figure 6. Registration phase of proposed scheme

5.3. Authentication Phase

When EV$_i$ wants to use the charging service, EV$_i$ and EAG must authenticate each other, and then generate a common session key. Figure 7 shows the authentication phase with detailed steps as follows

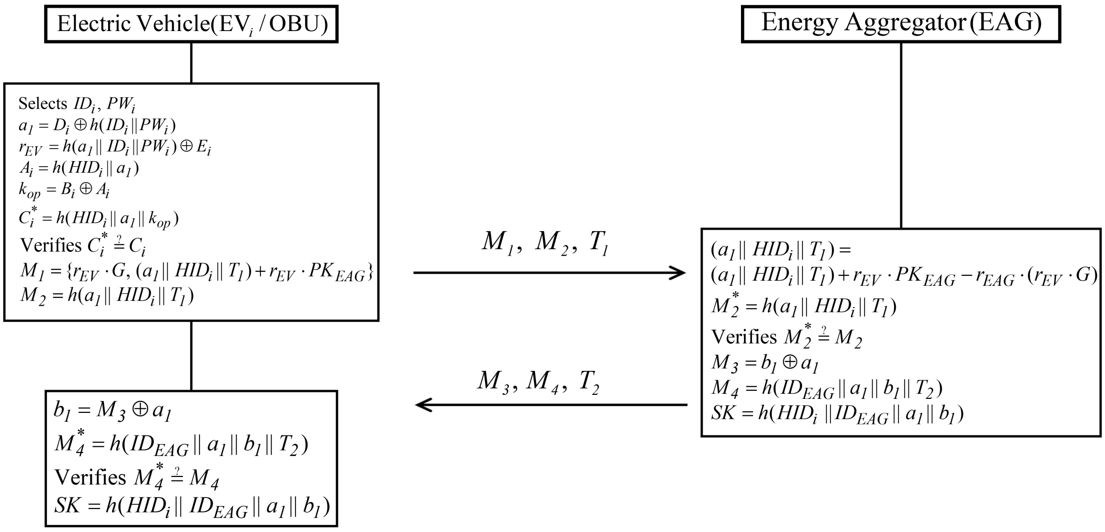

Electric Vehicle(EV$_i$ / OBU)
Energy Aggregator (EAG)
Selects ID_i, PW_i
$a_1 = D_i \oplus h(ID_i \| PW_i)$
$r_{EV} = h(a_1 \| ID_i \| PW_i) \oplus E_i$
$A_i = h(HID_i \| a_1)$
$k_{op} = B_i \oplus A_i$
$C_i^* = h(HID_i \| a_1 \| k_{op})$
Verifies $C_i^* \overset{?}{=} C_i$
$M_1 = \{r_{EV} \cdot G, (a_1 \| HID_i \| T_1) + r_{EV} \cdot PK_{EAG}\}$
$M_2 = h(a_1 \| HID_i \| T_1)$
M_1, M_2, T_1
$(a_1 \| HID_i \| T_1) =$
$(a_1 \| HID_i \| T_1) + r_{EV} \cdot PK_{EAG} - r_{EAG} \cdot (r_{EV} \cdot G)$
$M_2^* = h(a_1 \| HID_i \| T_1)$
Verifies $M_2^* \overset{?}{=} M_2$
$M_3 = b_1 \oplus a_1$
$M_4 = h(ID_{EAG} \| a_1 \| b_1 \| T_2)$
$SK = h(HID_i \| ID_{EAG} \| a_1 \| b_1)$
M_3, M_4, T_2
$b_1 = M_3 \oplus a_1$
$M_4^* = h(ID_{EAG} \| a_1 \| b_1 \| T_2)$
Verifies $M_4^* \overset{?}{=} M_4$
$SK = h(HID_i \| ID_{EAG} \| a_1 \| b_1)$

Figure 7. Authentication phase of proposed scheme.

Step 1: EV$_i$ inputs identity ID_i and password PW_i; and calculates $a_1 = D_i \oplus h(ID_i||PW_i)$, $r_{EV} = h(a_1||ID_i||PW_i) \oplus E_i$, $A_i = h(HID_i||a_i)$, $k_{op} = B_i \oplus A_i$, and $C_i^* = h(HID_i||a_1||k_{op})$. Then, EV$_i$ checks whether $C_i^* \overset{?}{=} C_i$. If valid, EV$_i$ computes $M_1 = \{r_{EV} \cdot G, (a_1||HID_i||T_i) + r_{EV} \cdot PK_{EAG}\}$, and $M_2 = h(a_1||HID_i||T_1)$; and sends $\{M_1, M_2, T_1\}$ to EAG.

Step 2: After receiving $\{M_1, M_2, T_1\}$ from EV$_i$, EAG calculates $(a_1||HID_i||T_1) = (a_1||HID_i||T_1) + r_{EV} \cdot PK_{EAG} - r_{EAG} \cdot (r_{EV} \cdot G)$ using the private key r_{EAG}. Then EAG computes $M_2^* = h(a_1||HID_i||T_1)$ and verifies $M_2^* \overset{?}{=} M_2$. If valid, EAG authenticates EV$_i$ and calculates $M_3 = b_1 \oplus a_1$, $M_4 = h(ID_{EAG}||a_1||b_1||T_2)$, and session key $SK = h(HID_i||ID_{EAG}||a_1||b_1)$. Finally, EAG sends $\{M_3, M_4, T_2\}$ to EV$_i$.

Step 3: When EV$_i$ receives $\{M_3, M_4, T_2\}$ from EAG, it computes $b_1 = M_3 \oplus a_1$ and $M_4^* = h(IE_{EAG}||a_1||b_1||T_2)$, and verifies $M_4^* \overset{?}{=} M_4$. If valid, mutual authentication between EV$_i$ and EAG has been accomplished. EV$_i$ calculates a shared session key, $SK = h(HID_i||ID_{EAG}||a_1||b_1)$.

5.4. Charging Phase

Charging commences after successfully completing authentication. Figure 8 shows the charging phase with detailed steps as follows.

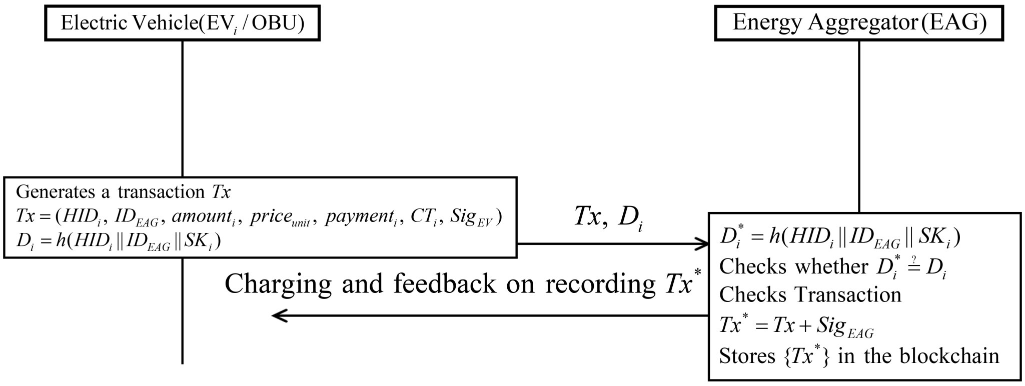

Electric Vehicle(EV_i / OBU)
Energy Aggregator (EAG)
Generates a transaction Tx
$Tx = (HID_i, ID_{EAG}, amount_i, price_{unit}, payment_i, CT_i, Sig_{EV})$
$D_i = h(HID_i \| ID_{EAG} \| SK_i)$
Tx, D_i
Charging and feedback on recording Tx^*
$D_i^* = h(HID_i \| ID_{EAG} \| SK_i)$
Checks whether $D_i^* \overset{?}{=} D_i$
Checks Transaction
$Tx^* = Tx + Sig_{EAG}$
Stores $\{Tx^*\}$ in the blockchain

Figure 8. Charging phase of proposed scheme.

Step 1: EV$_i$ generates a transaction T_x including HID_i; ID_{EAG}; charging records, prices, charging time CT_i, signature of EV$_i$ and information of payment, and EV$_i$ computes $D_i = h(HID_i||ID_{EAG}||SK_i)$. After that, EV$_i$ sends $\{T_x, D_i\}$ to the EAG.

Step 2: After receiving the message from EV$_i$, EAG checks whether $D_i^* \overset{?}{=} D_i$. If it is correct, EAG checks whether the transaction information T_x is correct. Then, EAG adds the own signature to the transaction. Finally, the charging is started and EAG records the transaction T_x on the blockchain.

6. Security Analysis

This section demonstrates that the proposed system is secure against various attacks using informal analysis and proves the system provides secure mutual authentication using BAN logic [34], a widely accepted formal security analysis. We also show it is secure against replay and man-in-the-middle attacks using automated validation of internet security protocols and applications (AVISPA) [35] which is a formal security verification tool.

6.1. Informal Security Analysis

We perform informal security analysis to evaluate the proposed system security, and show the system can resist impersonation, replay, perfect forward secrecy, and session key disclosure attacks; and also provides secure mutual authentication and anonymity.

6.1.1. Impersonation Attack

If adversary EV$_A$ attempts to impersonate a legitimate user EV$_i$, EV$_A$ must successfully generate a request message $M_2 = h(a_1||HID_i||T_1)$. However, EV$_A$ cannot calculate the request message because they cannot obtain EV$_i$'s random number a_1, and real identity ID_i. EV$_A$ also cannot obtain EV$_i$'s sensitive information because transmitted message M_1 is encrypted by EV$_i$. Therefore, the proposed protocol prevents impersonation attack.

6.1.2. Session Key Disclosure Attack

In the proposed system, the adversary EV$_A$ cannot generate a valid session key $h(HID_i||ID_{EAG}||a_1||b_1)$ because EV$_A$ cannot obtain EV$_i$'s real identity ID_i; or random numbers, a_1 and b_1, generated by EAG. EV$_A$ also cannot decrypt M_1 without EV$_i$'s private key r_{EV}. Therefore, the proposed protocol can resist session key disclosure attack.

6.1.3. Perfect Forward Secrecy

Even if an EV$_i$ long-term private parameter of EV$_i$ is compromised, EV$_A$ does not obtain the previous session key. Suppose the long-term private parameter a_1 is leaked. EV$_A$ cannot obtain ID_i because they cannot decrypt M_1 without the correct private key. Therefore, the proposed protocol guarantees perfect forward secrecy.

6.1.4. Replay Attack

Suppose EV$_A$ attempted a replay attack using previous transmitted messages. However, EV$_A$ cannot reuse previous messages, because all transmitted messages include timestamps, and EV$_i$ and EAG check all transmitted messages including the timestamps are correct. Therefore, the proposed protocol prevents replay attack.

6.1.5. Mutual Authentication

Sections 6.1.1 and 6.1.2 demonstrate that EV$_A$ cannot impersonate EV$_i$ and obtain the session key. All transmitted parameters are checked by EV$_i$ and EV$_A$. When EAG receives the request message $\{M_1, M_2, T_1\}$ from EV$_i$, EAG decrypts M_1 using its own private key, and verifies M_2. If valid, EAG authenticates EV$_i$. When EV$_i$ receives response $\{M_3, M_4, T_2\}$ from EAG, it computes $b_1 = M_3 \oplus h(HID_i||a_1)$ and $M_4^* = h(ID_{EAG}||a_1||b_1||T_2)$, and then verifies $M_4^* = h(ID_{EAG}||a_1||b_1||T_2)$. If valid, EV$_i$ authenticates EAG. Therefore, the proposed system provides secure mutual authentication because EV$_i$ and EAG successfully authenticate each other using private keys.

6.1.6. Anonymity

Suppose EV$_A$ intercepts all previous transmitted messages to attempt to obtain EV$_i$'s real identity. However, all EV$_i$ parameters, including ID_i, are masked by hash or encryption. Therefore, the proposed protocol ensures anonymity.

6.2. Security Analysis Using BAN Logic

We perform a security analysis using BAN logic to demonstrate the proposed system provides secure mutual authentication between EV and EAG. Table 2 introduces BAN logic notations and defines the goals, rules, idealized forms, and assumptions to perform BAN logic analysis.

Table 2. Notations for BAN logic.

Notation	Description
$A\| \equiv X$	A **believes** statement X
#X	Statement X is **fresh**
$A \lhd X$	A **sees** statement X
$A\| \sim X$	A once **said** X
$A \Rightarrow X$	A **controls** statement X
$< X >_Y$	Formula X is **combined** with formula Y
$\{X\}_K$	X is **encrypted** under key K
$A \overset{K}{\leftrightarrow} B$	A and B may use **shared key** K to communicate
$\overset{K}{\longrightarrow}_B$	B has K as a **public key**
SK	Session key used in the current session

BAN Logic Rules

The BAN logic rules are as follows.

1. Message meaning rule :

$$\frac{A \Big| \equiv A \overset{K}{\leftrightarrow} B, \quad A \lhd \{X\}_K}{A \ |\equiv B \mid \sim X}$$

2. Nonce verification rule :

$$\frac{A \ |\equiv \#(X), \quad A \mid \equiv B \Big| \sim X}{A \ |\equiv B \mid \equiv X}$$

3. Jurisdiction rule :

$$\frac{A \ |\equiv B \mid \Longrightarrow X, \quad A \ |\equiv B \mid \equiv X}{A \Big| \equiv X}$$

4. Freshness rule :

$$\frac{A \Big| \equiv \#(X)}{A \Big| \equiv \#(X, Y)}$$

5. Belief rule :

$$\frac{A \Big| \equiv (X, Y)}{A \Big| \equiv X.}$$

6.3. Goals

We define the following security goals to prove the proposed system ensures secure mutual authentication.

Goal 1: $EV \ |\equiv (EV \overset{SK}{\longleftrightarrow} EAG)$

Goal 2: $EV \ |\equiv EAG \ |\equiv (EV \overset{SK}{\longleftrightarrow} EAG)$

Goal 3: $EAG \ |\equiv (EV \overset{SK}{\longleftrightarrow} EAG)$

Goal 4: $EAG \ |\equiv EV \ |\equiv (EV \overset{SK}{\longleftrightarrow} EAG)$

6.3.1. Idealized Forms

The idealized forms are given below.

Msg_1: $EV \rightarrow EAG$: $(a_1, HID_i, T_1) \overset{PK_{EAG}}{\longrightarrow_{EAG}}$

Msg_2: $EAG \rightarrow EV$: $(b_1, ID_{EAG}, T_2)_{a_1}$

6.3.2. Assumptions

We define the following initial assumptions for the BAN logic proof.

A_1: $EAG \ |\equiv \#(T_1)$

A_2: $EV \ |\equiv \#(T_2)$

A_3: $EV \ |\equiv (EAG \overset{a_1}{\longleftrightarrow} EV)$

A_4**:** $EAG \mid\equiv \#(PK_{EAG})$

A_5**:** $EAG \mid\equiv \#(a_1)$

A_6**:** $EV \mid\equiv \#(b_1)$

A_7**:** $EV \mid\equiv EAG \Rightarrow (EV \overset{SK}{\longleftrightarrow} EAG)$

A_8**:** $EAG \mid\equiv EV \Rightarrow (EV \overset{SK}{\longleftrightarrow} EAG)$

6.3.3. Proof using BAN Logic

The detailed steps of the BAN logic proof are as follows.

Step 1: From Msg_1,

$$S_1 : EAG \lhd (a_1, HID_i, T_1) \overset{PK_{EAG}}{\longrightarrow}_{EAG}$$

Step 2: From the message meaning rule with S_1 and A_4,

$$S_2 : EAG \mid\equiv EV \sim (a_1, HID_i, T_1)$$

Step 3: Using the freshness rule with A_1,

$$S_3 : EAG \mid\equiv \#(a_1, HID_i, T_1)$$

Step 4: From the nonce verification rule with S_2 and S_3,

$$S_4 : EAG \mid\equiv EV \mid\equiv (a_1, HID_i, T_1)$$

Step 5: Since the session key $SK = h(HID_i||ID_{EAG}||a_1||b_1)$, from S_4 and A_5,

$$S_5 : EAG \mid\equiv EV \mid\equiv (EV \overset{SK}{\longleftrightarrow} EAG) \qquad \textbf{(Goal 4)}$$

Step 6: From the jurisdiction rule with S_6 and A_8,

$$S_6 : EAG \mid\equiv (EV \overset{SK}{\longleftrightarrow} EAG) \qquad \textbf{(Goal 3)}$$

Step 7: From the Msg_2,

$$S_7 : EV \lhd (b_1, ID_{EAG}, T_2)_{a_1}$$

Step 8: Using the message meaning rule with S_8 and A_3,

$$S_8 : EV \mid\equiv EAG \sim (b_1, ID_{EAG}, T_2)_{a_1}$$

Step 9: From the freshness rule with A_2,

$$S_9 : EV \mid\equiv \#(b_1, ID_{EAG}, T_2)_{a_1}$$

Step 10: From the nonce verification rule with S_9 and S_{10},

$$S_{10} : EV \mid\equiv EAG \mid\equiv (b_1, ID_{EAG}, T_2)_{a_1}$$

Step 11: Since the session key $SK = h(HID_i||ID_{EAG}||a_1||b_1)$, from S_{11} and A_6,

$$S_{11} : EV \mid\equiv EAG \mid\equiv (EV \overset{SK}{\longleftrightarrow} EAG) \qquad \textbf{(Goal 2)}$$

Step 12: From the jurisdiction rule with S_{13} and A_7,

$$S_{12} : EV \mid\equiv (EV \overset{SK}{\longleftrightarrow} EAG) \qquad \textbf{(Goal 1)}$$

Therefore, the proposed protocol achieves secure mutual authentication between EV and EAG.

6.4. Formal Security AVISPA Tool for Formal Security Verification

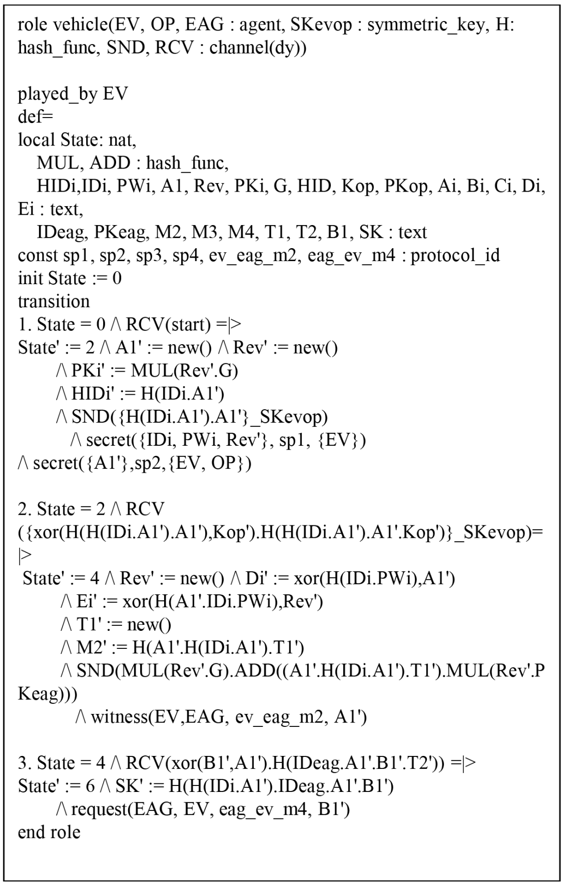
To prove the proposed system is secure against replay and man-in-the-middle attacks, we performed formal security analysis using AVISPA [35], a widely accepted formal security verification tool to check systems or protocols can resist replay and man-in-the-middle attacks [36–39].

The AVISPA module was written in a high level protocol specification language (HLPSL) [40] and consists of four backends: Tree Automate-based Protocol Analyser (TA4SP), SAT-based Model-Checker (SATMC), CL-based Attack Searcher(CL-AtSe) [41] and On-the-Fly Model-Checker(OFMC) [42]. Detailed AVISPA and HLPSL are presented in [35,40].

6.4.1. HLPSL Specification of AVISPA Simulation

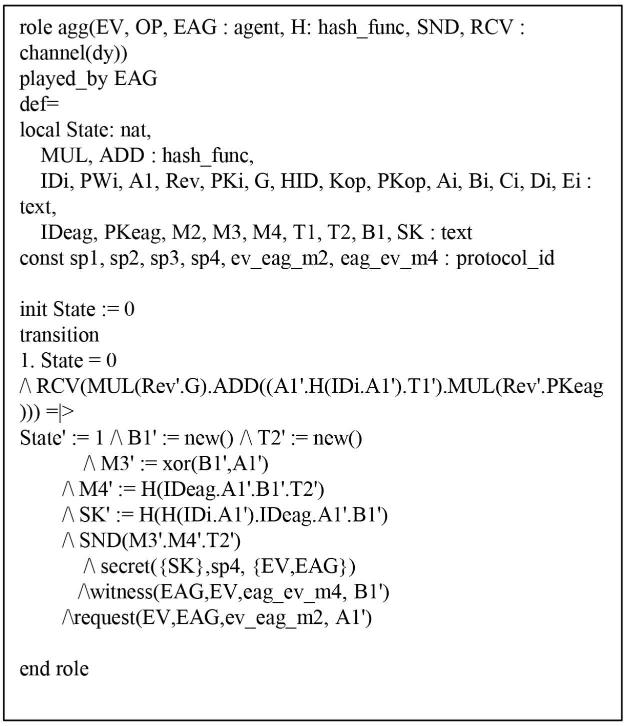
The HLPSL consists of three components: *role*, *session*, and *environment*, where *role* denotes entity, *session* includes system parameters, and *environment* includes intruder knowledge, security goal and authentication goal. Figures 9–11 show HLPSL specifications for EV, EAG, and OP, respectively. Figure 12 shows *session* and *environment* roles.

Figure 9 shows the *role* for EV. In state 0, EV receives the start request and performs registration. EV sends the registration request $\{HID_i, a_1\}$ to OP via a secure channel, updates the state value to 2, and then checks whether the entity is a legitimate user using the *secret* function.



```
role vehicle(EV, OP, EAG : agent, SKevop : symmetric_key, H:
hash_func, SND, RCV : channel(dy))

played_by EV
def=
local State: nat,
   MUL, ADD : hash_func,
   HIDi,IDi, PWi, A1, Rev, PKi, G, HID, Kop, PKop, Ai, Bi, Ci, Di,
Ei : text,
   IDeag, PKeag, M2, M3, M4, T1, T2, B1, SK : text
const sp1, sp2, sp3, sp4, ev_eag_m2, eag_ev_m4 : protocol_id
init State := 0
transition
1. State = 0 /\ RCV(start) =|>
State' := 2 /\ A1' := new() /\ Rev' := new()
       /\ PKi' := MUL(Rev'.G)
       /\ HIDi' := H(IDi.A1')
       /\ SND({H(IDi.A1').A1'}_SKevop)
         /\ secret({IDi, PWi, Rev'}, sp1, {EV})
/\ secret({A1'},sp2,{EV, OP})

2. State = 2 /\ RCV
({xor(H(H(IDi.A1').A1'),Kop').H(H(IDi.A1').A1'.Kop')}_SKevop)=
|>
 State' := 4 /\ Rev' := new() /\ Di' := xor(H(IDi.PWi),A1')
        /\ Ei' := xor(H(A1'.IDi.PWi),Rev')
        /\ T1' := new()
        /\ M2' := H(A1'.H(IDi.A1').T1')
        /\ SND(MUL(Rev'.G).ADD((A1'.H(IDi.A1').T1').MUL(Rev'.P
Keag)))
           /\ witness(EV,EAG, ev_eag_m2, A1')

3. State = 4 /\ RCV(xor(B1',A1').H(IDeag.A1'.B1'.T2')) =|>
State' := 6 /\ SK' := H(H(IDi.A1').IDeag.A1'.B1')
       /\ request(EAG, EV, eag_ev_m4, B1')
end role
```

Figure 9. Specification of the electronic vehicle.

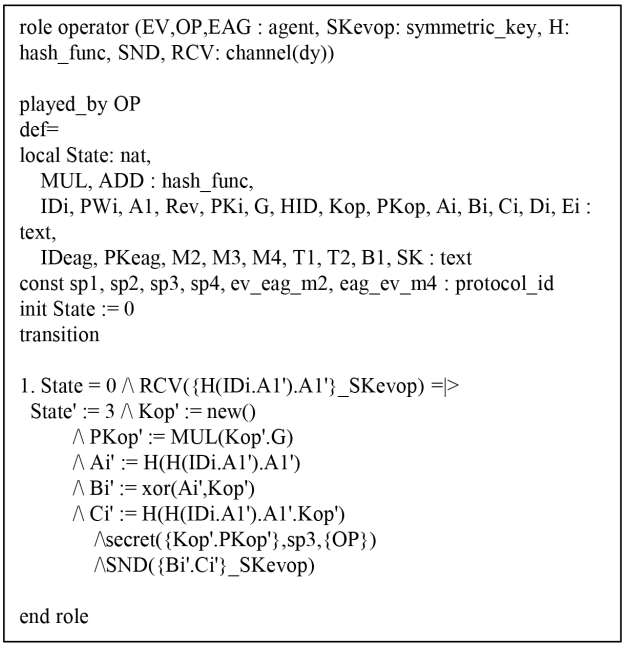


```
role agg(EV, OP, EAG : agent, H: hash_func, SND, RCV :
channel(dy))
played_by EAG
def=
local State: nat,
   MUL, ADD : hash_func,
   IDi, PWi, A1, Rev, PKi, G, HID, Kop, PKop, Ai, Bi, Ci, Di, Ei :
text,
   IDeag, PKeag, M2, M3, M4, T1, T2, B1, SK : text
const sp1, sp2, sp3, sp4, ev_eag_m2, eag_ev_m4 : protocol_id

init State := 0
transition
1. State = 0
/\ RCV(MUL(Rev'.G).ADD((A1'.H(IDi.A1').T1').MUL(Rev'.PKeag
))) =|>
State' := 1 /\ B1' := new() /\ T2' := new()
         /\ M3' := xor(B1',A1')
      /\ M4' := H(IDeag.A1'.B1'.T2')
      /\ SK' := H(H(IDi.A1').IDeag.A1'.B1')
      /\ SND(M3'.M4'.T2')
         /\ secret({SK},sp4, {EV,EAG})
        /\witness(EAG,EV,eag_ev_m4, B1')
      /\request(EV,EAG,ev_eag_m2, A1')

end role
```

Figure 10. Specification of the energy aggregator.

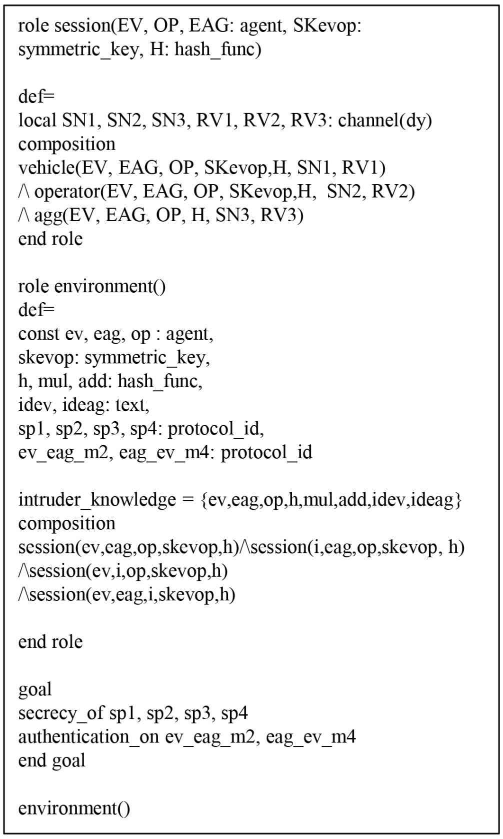
In state 4, EV receives response $\{B_i, C_i\}$ from OP through a secure channel and sends the login request $\{M_1, M_2, T_1\}$ to EAG via an open channel. EV also declares $witness(\mathrm{EV}, \mathrm{EAG}, ev\_eag\_m2, A1')$ to prove that a_1 is a weakness authentication factor. EV receives the response $\{M_3, M_4, T_2\}$ from OP, and then calculates the session key and updates the state value to 6.

In state 6, EV declares $request(\mathrm{EAG}, \mathrm{EV}, egg_e v_m 4, B1')$ to authenticate each other. The HLPSL specifications for EAG and OP roles are described similarly (see Figures 10 and 11).



```
role operator (EV,OP,EAG : agent, SKevop: symmetric_key, H:
hash_func, SND, RCV: channel(dy))

played_by OP
def=
local State: nat,
   MUL, ADD : hash_func,
   IDi, PWi, A1, Rev, PKi, G, HID, Kop, PKop, Ai, Bi, Ci, Di, Ei :
text,
   IDeag, PKeag, M2, M3, M4, T1, T2, B1, SK : text
const sp1, sp2, sp3, sp4, ev_eag_m2, eag_ev_m4 : protocol_id
init State := 0
transition

1. State = 0 /\ RCV({H(IDi.A1').A1'}_SKevop) =|>
 State' := 3 /\ Kop' := new()
       /\ PKop' := MUL(Kop'.G)
       /\ Ai' := H(H(IDi.A1').A1')
       /\ Bi' := xor(Ai',Kop')
       /\ Ci' := H(H(IDi.A1').A1'.Kop')
          /\secret({Kop'.PKop'},sp3,{OP})
          /\SND({Bi'.Ci'}_SKevop)

end role
```

Figure 11. Specification of the operator.

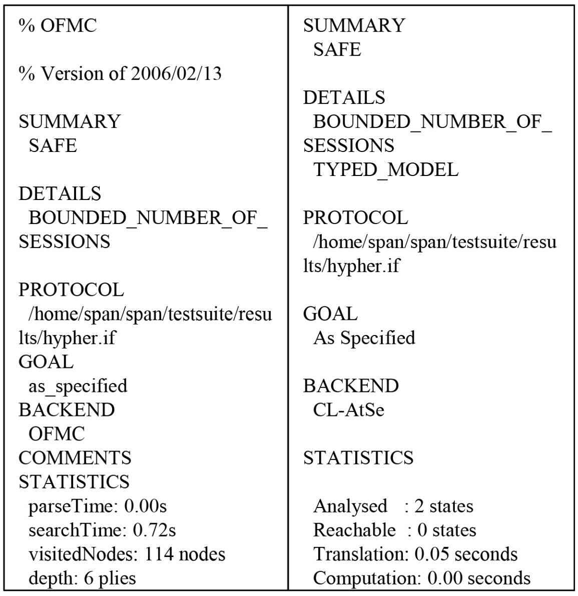


```
role session(EV, OP, EAG: agent, SKevop:
symmetric_key, H: hash_func)

def=
local SN1, SN2, SN3, RV1, RV2, RV3: channel(dy)
composition
vehicle(EV, EAG, OP, SKevop,H, SN1, RV1)
/\ operator(EV, EAG, OP, SKevop,H,  SN2, RV2)
/\ agg(EV, EAG, OP, H, SN3, RV3)
end role

role environment()
def=
const ev, eag, op : agent,
skevop: symmetric_key,
h, mul, add: hash_func,
idev, ideag: text,
sp1, sp2, sp3, sp4: protocol_id,
ev_eag_m2, eag_ev_m4: protocol_id

intruder_knowledge = {ev,eag,op,h,mul,add,idev,ideag}
composition
session(ev,eag,op,skevop,h)/\session(i,eag,op,skevop, h)
/\session(ev,i,op,skevop,h)
/\session(ev,eag,i,skevop,h)

end role

goal
secrecy_of sp1, sp2, sp3, sp4
authentication_on ev_eag_m2, eag_ev_m4
end goal

environment()
```

Figure 12. Specification of the session.

6.4.2. AVISPA Verification Results

We used AVISPA with security protocol animator (SAPN) [43] to evaluate whether the proposed system was secure against replay and man-in-the-middle attacks. HLPSL is translated to intermediate format (IF) and the simulation results are presented in output format (OF). OFMC and CL-AtSe check whether our proposed system prevent replay and man-in-the-middle attacks. Figure 13 shows that OFMC backend visited 114 nodes with 0.72 s search time, and CL-AtSe backend analyzed the 2 states with 0.05 s translation time.



```
% OFMC

% Version of 2006/02/13

SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_
SESSIONS

PROTOCOL
  /home/span/span/testsuite/resu
lts/hypher.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.72s
  visitedNodes: 114 nodes
  depth: 6 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_
SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/resu
lts/hypher.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 2 states
  Reachable  : 0 states
  Translation: 0.05 seconds
  Computation: 0.00 seconds
```

Figure 13. AVISPA simulation results.

7. Performance Analysis

This section compares the proposed system computation and communication costs with related schemes [20,44,45]. Figures 14–16 present the actual data workflow transmitted on our system to help understand the results of performance analysis. In Figure 14, operator provides the data for scheduling to EV and consensus nodes on blockchain verifty the validity of transactions.

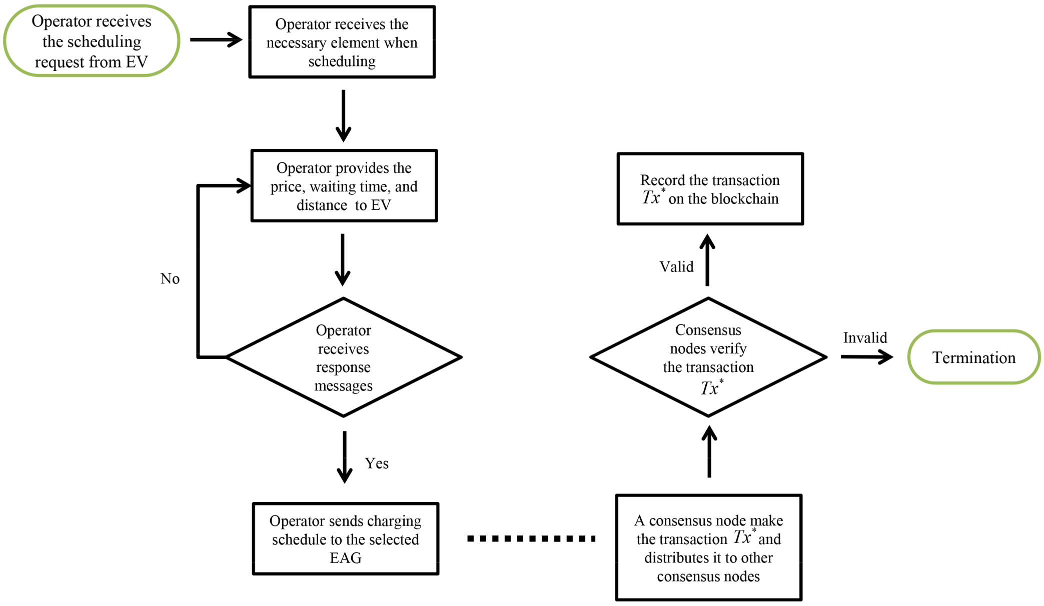

Operator receives the scheduling request from EV
Operator receives the necessary element when scheduling
Operator provides the price, waiting time, and distance to EV
No
Operator receives response messages
Yes
Operator sends charging schedule to the selected EAG
A consensus node make the transaction Tx^* and distributes it to other consensus nodes
Consensus nodes verify the transaction Tx^*
Valid
Record the transaction Tx^* on the blockchain
Invalid
Termination

Figure 14. Actual data workflow of network.

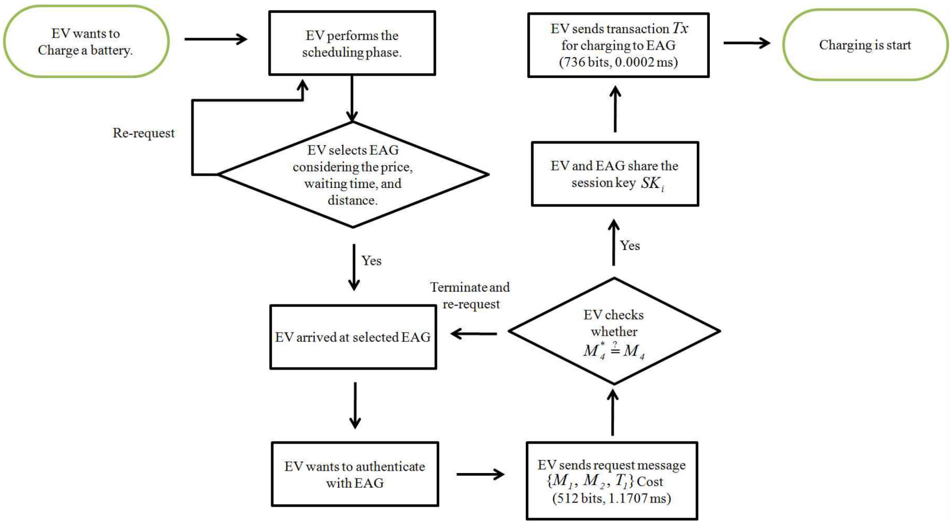

EV wants to Charge a battery.
EV performs the scheduling phase.
Re-request
EV selects EAG considering the price, waiting time, and distance.
Yes
EV arrived at selected EAG
EV wants to authenticate with EAG
EV sends request message $\{M_1, M_2, T_1\}$ Cost (512 bits, 1.1707 ms)
EV checks whether $M_4^* \overset{?}{=} M_4$
Terminate and re-request
Yes
EV and EAG share the session key SK_i
EV sends transaction Tx for charging to EAG (736 bits, 0.0002 ms)
Charging is start

Figure 15. Actual data workflow of EV.

7.1. Computation Cost

We compare computation overheads for the proposed system with related schemes [20,44,45], using the parameters from [46,47].

- Bilinear pairing,$T_{bp} = 4.211$ms.
- Scalar multiplication with bilinear pairing,$T_{sm-bp} = 1.709$ ms.
- Point addition with bilinear pairing, $T_{pa-bp} = 0.007$ ms.
- Scalar multiplication with elliptic curve cryptography, $T_{sm-ecc} = 0.442$ ms.
- Point addition with elliptic curve cryptography, $T_{pa-ecc} = 0.0018$ ms.
- Encryption with elliptic curve cryptography, $T_{enc-ecc} = 1.17$ ms.

- Decryption with elliptic curve cryptography, $T_{dec-ecc} = 0.61$ ms.
- Hash, $T_h = 0.0001$ ms.
- Map-to-point,$T_{mtp} = 4.302$ ms.

Table 3 compares computation costs for the considered schemes. In Figure 15, the EV's computation costs of our system are (1.1707 + 0.0002 = 1.1709 ms), including $T_{enc-ecc}$ and $9T_h$. In Figure 16, the EAG's computation costs of our system are (0.6103 + 0.0001 = 0.6104 ms), including $T_{dec-ecc}$ and $4T_h$.

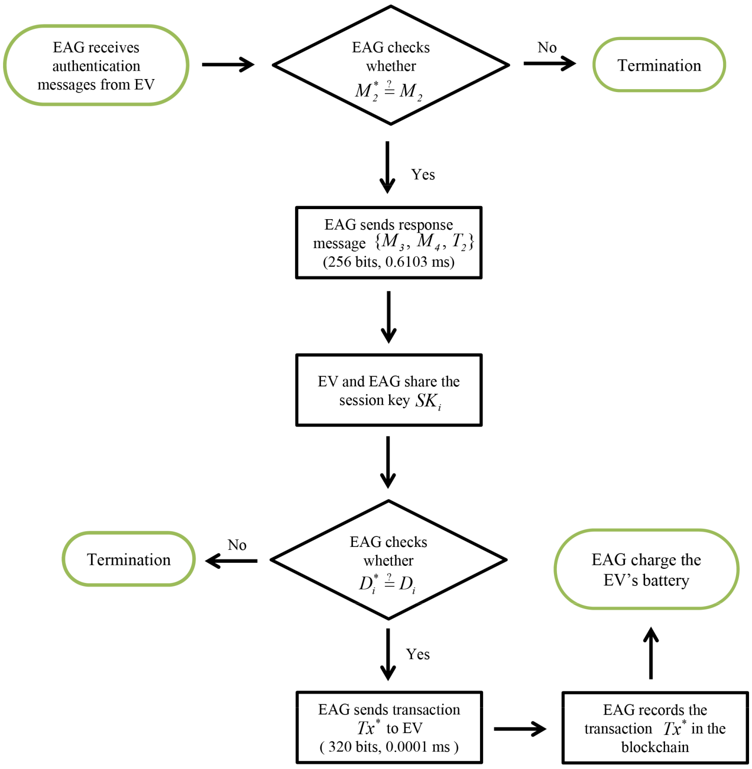

EAG receives authentication messages from EV
EAG checks whether $M_2^* \overset{?}{=} M_2$
No
Termination
Yes
EAG sends response message $\{M_3, M_4, T_2\}$ (256 bits, 0.6103 ms)
EV and EAG share the session key SK_i
Termination
No
EAG checks whether $D_i^* \overset{?}{=} D_i$
EAG charge the EV's battery
Yes
EAG sends transaction Tx^* to EV (320 bits, 0.0001 ms)
EAG records the transaction Tx^* in the blockchain

Figure 16. Actual data workflow of EAG.

In Huang et al.'s system [20], EV's total computation costs are (0.4459 + 0.0001 = 0.4460 ms), including T_{sm-ecc}, $2T_{pa-ecc}$ and $4T_h$. EAG's total computation cost is 0.8882 ms, including $2T_{sm-ecc}$, $2T_{pa-ecc}$ and $7T_h$.

The total cost for the proposed and Huang et al.'s scheme = 1.7811 and 1.3343 ms , respectively. Although the proposed protocol computation cost of somewhat higher than the Huang et al.'s scheme, it provides better efficiency and security than other related schemes.

Table 3. Computation costs for related schemes.

	Lai et al. [44]	Qiu et al. [45]	Huang et al. [20]	Proposed
EV	$7T_{sm-bp} + T_{pa-bp} + T_{mtp}$ ≈ 16.272 ms	$2T_{sm-ecc} + 3T_{pa-ecc} + 8T_h$ ≈ 0.8902 ms	$T_{sm-ecc} + 2T_{pa-ecc} + 4T_h$ ≈ 0.4460 ms	$T_{enc-ecc} + 9T_h$ ≈ 1.1709 ms
EAG	$2T_{bp} + 5T_{sm-bp} + T_{pa-bp} + T_{mtp}$ ≈ 21.276 ms	$2T_{sm-ecc} + 4T_{pa-ecc} + 5T_h$ ≈ 0.8917 ms	$2T_{sm-ecc} + 2T_{pa-ecc} + 7T_h$ ≈ 0.8883 ms	$T_{dec-ecc} + 4T_h$ ≈ 0.6104 ms

7.2. Communication Cost

We compare communication overheads for the proposed system with related schemes [20,44,45]. We assume timestamp, random number and identity are 32, 64, and 128 bits, respectively [48–50]; and elliptic curve cryptography encryption and hash function are 320 and 160 bits, respectively. For the proposed system, we assume group G is generated by P with order q on elliptic curve cryptography $y^2 = x^3 + ax + b$ mod p, where p and q are 160 bits prime numbers. Similarly, G_1, G_2, and G are 1024, 160, and 320 bits, respectively. In Figure 15, the EV's communication costs of our system are (512 + 736 = 1248 bits), including charging request messages $\{M_1, M_2, T_1\}$ and transaction T_x. In Figure 16, the EAG's communication costs of our system are (256 + 320 = 576 bits), including response messages $\{M_3, M_4, T_2\}$ and transaction T_x^*.

In Huang et al.'s system [20], EV's total communication costs are (2368 + 160 = 2528 bits), including charging requset messages $\{ID_{CP}, Q_{CP}, P_{CP}, K\}$, response messages $\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \zeta_{EV}\}$ and charging request messages $H_5(ID_{EV}, R_{CP}, \zeta_{CP}, P)$. EAG's total communication costs are 1760 bits, including response messages $\{PID_{EV}, Q_{EV}, T_{EV}, SK_{EV}\}$ and $\{ID_{EV}, PID_{EV}, R_{CP}, \zeta_{CP}\}$.

Table 4 shows communication cost results for all considered schemes. More particularly, the communication cost is efficient compared with other schemes in view of EVs. It is a very important advantage because EV is equipped with resourse-constrained devices as sensors. Thus, the proposed system provides more efficient communication than all other considered schemes.

Table 4. Communication costs.

Scheme	Total Messages	Communication Cost
Lai et al. [44]	2	2560 bits
Qiu et al. [45]	3	2656 bits
Huang et al. [20]	5	4288 bits
Proposed	4	1824 bits

8. Conclusions

With the rapid development of the IoT and embedded technologies, drivers can access various services. However, these services are vulnerable to potential attacks such as replay, impersonation and session key disclosure attacks because they are provided through public channels. Many traditional cryptographic algorithms such as RSA also are suitable to vehicular networks because a vehicle is equipped with resource-constrained sensors. Therefore, secure mutual authentication and key agreement are very important security requirements to guarantee privacy of users, considering the resource-constrained sensors.

This paper demonstrated that Huang et al.'s scheme does not provide high efficiency and security of keys, and has various authentication flaws, including excess deposits, inefficient transaction generation, and excess transaction fees. We proposed a secure charging system for electric vehicles based on blockchain to address these weaknesses, providing high efficiency, anonymity, perfect forward secrecy, and secure mutual authentication. We demonstrated that the proposed system prevents impersonation, session key disclosure, and replay attacks, proved secure mutual authentication between EV and EAG using BAN logic, and confirmed resistance to replay and man-in-the-middle attacks using AVISPA. We compared computation and communication costs with related schemes, and showed that the proposed scheme was superior to all considered schemes. Thus, the proposed system could be applied to IoT-based practical EV charging systems for resource-constrained devices.

Author Contributions: Conceptualization, M.K.; Formal analysis, K.P. and S.Y.; Software, J.L.; Supervision, Y.P.; Validation, K.P. and Y.P.; Writing—original draft, M.K.; Writing—review & editing, K.P., S.Y., Y.P., S.-W.L. and B.C.

Funding: This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00312, Developing technologies to predict, detect, respond, and automatically diagnose security threats to automotive Ethernet-based vehicle).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cheung, V. South Korea Releases Electric Public Transportation System. Available online: http://globalenergyinitiative.org/south-koreareleases-electric-public-transportation-system.html (accessed on 11 May 2019).
2. Lo, N.-W.; Tasi, J.-L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Trans. Intell. Transport. Syst.* **2016**, *17*, 1319–1328. [CrossRef]
3. Kumari, S.; Karuppiah, M.; Li, X.; Wu, F.; Das, A.K. An enhanced and secure trust-extended authentication mechanism for vehicular ad-hoc networks. *Secur. Commun. Netw.* **2016**, *9*, 4255–4271. [CrossRef]
4. Chin, W.-L.; Li, W.; Chen, H.-H. Energy big data security threats in IoT-based smart grid communications. *IEEE Commun. Mag.* **2017**, *55*, 70–75. [CrossRef]
5. Liu, Y.; Wang, Y.; Chang, G. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. *IEEE Trans. Intell. Transport. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
6. Mohit P.; Amin, R.; Biswas, G.P. Design of authentication protocol for wireless sensor network-based smart vehicular system. *Veh. Commun.* **2017**, *9*, 64–71. [CrossRef]
7. Guo, L.; Dong, M.; Ota, K.; Li, Q.; Ye, T.; Wu, J. ; Li, J. A secure mechanism for big data collection in large scale internet of vehicle. *IEEE Internet Things J.* **2017**, *4*, 601–610 [CrossRef]
8. Zhou, Y.; Zhao, X.; Jiang, Y.: Shang, F.; Deng, S.; Wang, X. An enhanced privacy-preserving authentication scheme for vehicle sensor networks. *Sensors* **2017**, *17*, 2854–2877. [CrossRef]
9. 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*, 2526–2536. [CrossRef]
10. Wu, L.; Sun, Q.; Wang, X.; Wang, J.; Yu, S.; Zou, Y.; Liu, B.; Zhu, Z. An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network. *IEEE Access* **2019**, *7*, 55050–55063. [CrossRef]
11. Gan, L.; Topcu, U.; Low, S.H. Optimal decentralized protocol for electric vehicle charging. *IEEE Trans. Power Syst.* **2013**, *28*, 940–951. [CrossRef]
12. Xu, Y.; Pan, F.; Tong, L. Dynamic Scheduling for Charging Electric Vehicles: A Priority Rule. *IEEE. Trans. Autom. Control* **2016**, *61*, 4094–4099. [CrossRef]
13. Lu, J.L.; Yeh, M.Y.; Hsu, Y.C.;Yang, S.N.; Gan, C.H.; Chen, M.S. Operating electric taxi fleets: A new dispatching strategy with charging plans. In Proceedings of the 2012 IEEE International Electric Vehicle Conference, Greenville, SC, USA, 4–8 March 2012; pp. 1–8.
14. Kim, H.J.; Lee, J.; Park, G.L.; Kang, M.J.; Kang, M. An efficient scheduling scheme on charging stations for smart transportation. In Proceedings of the International Conference on Security-Enriched Urban Computing and Smart Grid, Daejeon, Korea, 15–17 September 2010; pp. 274–278.
15. Tian, Z.; Jung, T.; Wang, Y.; Zhang, F.; Tu, L.; Xu, C.; Tian, C.; Li, X. Real-time charging station recommendation system for electric-vehicle taxis. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 3098–3109. [CrossRef]
16. Tang, W.; Zhang, Y.J.A. A model predictive control approach for lowcomplexity electric vehicle charging scheduling: Optimality and scalability. *IEEE Trans. Power Syst.* **2016**, *32*, 1050–1063. [CrossRef]
17. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 27 May 2019).
18. Pub, N.F. Secure Hash Standard. Available online: https://csrc.nist.gov/csrc/media/publications/fips/180/\2/archive/2002-08-01/documents/fips180-2withchangenotice.pdf (accessed on 27 May 2019).
19. Available online: https://www.hyperledger.org/resources/publications#white-papers (accessed on 27 May 2019).
20. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–313574. [CrossRef]
21. Poon, J.; Dryja, T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Available online: http://www.theblockchain.com/docs/Lightning%20Network (accessed on 27 May 2019).
22. Surhone, L.M.; Timpledon, M.T.; Marseken, S.F. *Smart Contract*; Betascript publishing: Saarbrücken, Germany, 2010; pp. 1–72, ISBN 978-613-0-48941-0.
23. Roman, R.; Alcaraz, C.; Lopez, J.; Sklavos, N. Key management systems for sensor networks in the context of the Internet of Things. *Comput. Electr. Eng.* **2011**, *37*, 147–159. [CrossRef]

24. Turkanovic, M.; Brumen, B.; Hölbl, 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 Netw.* **2014**, *20*, 96–112. [CrossRef]
25. Amin, R.; Biswas, G. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Netw.* **2016**, *36*, 58–80. [CrossRef]
26. Lu, Y.; Li, L.; Peng, H.; Yang, Y. An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks. *Sensors* **2016**, *16*, 837. [CrossRef]
27. Magazzeni, D.; McBurney, P.; Nash, W. Validation and verification of smart contracts: A research agenda. *Computer* **2017**, *50*, 50–57. [CrossRef]
28. Dubois, A.; Wehenkel, A.; Fonteneau, R.; Olivier, F.; Ernst, D. An app-based algorithmic approach for harvesting local and renewable energy using electric vehicles. In Proceedings of the 9th International Conference on Agents and Artificial Intelligence, Porto, Protugal, 24–26 February 2017; pp. 322–327.
29. Knirsch, F.; Unterweger, A.; Engel, D. Privacy-preserving blockchain based electric vehicle charging with dynamic tariff decisions. *Comput. Sci. Res. Dev.* **2017**, *33*, 71–79. [CrossRef]
30. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inf.* **2017**, *14*, 3690–3700. [CrossRef]
31. Wazid, M.; Das, A.K.; Kumar, N.; Odelu, V.; Reddy, A.G.; Park, K.; Park, Y. Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. *IEEE Access* **2017**, *5*, 14966–14980. [CrossRef]
32. Messerges, T.S.; Dabbish, E.A.; Sloan, R.H. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* **2002**, *51*, 541–552. [CrossRef]
33. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Proceedings of the Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, USA, 15–19 August 1999; pp. 388–397.
34. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication, *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36.
35. AVISPA. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispaproject.org/ (accessed on 10 May 2019).
36. Park, K.; Park, Y.; Park, Y.; Reddy, A.G.; Das, A.K.; Provably secure and efficient authentication protocol for roaming service in global mobility networks. *IEEE Access* **2017**, *5*, 25110–25125. [CrossRef]
37. Park, K.; Park, Y.; Park, Y.; Das, A.K. 2PAKEP: Provably secure and efficient two-party authenticated Key exchange protocol for mobile environment. *IEEE Access* **2018**, *6*, 30225–30241. [CrossRef]
38. Yu, S.; Lee, J.; Lee, K.; Park, K.; Park, Y. Secure authentication protocol for wireless sensor networks in vehicular communications. *Sensors* **2018**, *18*, 3191. [CrossRef]
39. Odelu, V.; Das, A.K.; Choo, K.R; Kumar, N.; Park, Y.; Efficient and secure time-key based single sign-on authentication for mobile devices. *IEEE Access* **2017**, *5*, 27707–27721. [CrossRef]
40. von Oheimb, D. The high-level protocol specification language HLPSL developed in the EU project avispa. In Proceedings of the APPSEM 2005 Workshop, Tallinn, Finland, 13–15 September 2005; pp. 1–2.
41. Turuani, M. The CL-Atse protocol analyser. In Proceedings of the 17th International Conference on Rewriting Techniques and Applications (RTA), Seattle, WA, USA, 12–14 August 2006; pp.277–286.
42. Basin, D.; Modersheim, S.; Vigano, L. OFMC: A symbolic model checker for security protocols. *Int. J. Inf. Secur.* **2005**, *4*, 181–208. [CrossRef]
43. SPAN: A Security Protocol Animator for AVISPA. Available online: http://www.avispa-project.org/ (accessed on 4 May 2019).
44. Lai, C.; Lu, R.; Li, H.; Zheng, D.; Shen, X.S. Secure machine-type communications in LTE networks. *Wirel. Commun. Mob. Comput.* **2016**, *16*, 1495–1509. [CrossRef]
45. Qiu, Y.; Ma, M.; Wang, X. A proxy signature-based handover authentication scheme for LTE wireless networks. *J. Netw. Comput. Appl.* **2017**, *83*, 63–71. [CrossRef]
46. Islam, S.K.H.; Obaidat, M.S.; Vijayakumar, P.; Abdulhay, E.; Li, F.; Reddy, M.K.C. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Future Gener. Comput. Syst.* **2018**, *84*, 216–227. [CrossRef]
47. Nkenyereye, L.; Kwon, J.; Choi, Y. Secure and lightweight cloud-assisted video reporting protocol over 5G-enabled vehicular networks. *Sensors* **2017**, *17*, 2191. [CrossRef] [PubMed]
48. Lee, H.; Lee, D.; Moon, J.; Jung, J.; Kang, D.; Kim, H.; Won, D. An improved anonymous authentication scheme for roaming in ubiquitous networks. *PLoS ONE* **2018**, *13*, e0193366. [CrossRef]

49. Yu, Y.; Li, Y.; Du, X.; Chen, R.; Yang, B. Content protection in named data networking: Challenges and potential solutions. *IEEE Commun. Mag.* **2018**, *56*, 82–87. [CrossRef]
50. Ying, B.; Nayak, A. Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography. *J. Netw. Comput. Appl.* **2019**, *131*, 66–74. [CrossRef]