Received January 26, 2018, accepted February 28, 2018, date of publication March 5, 2018, date of current version March 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2812176

LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem

XIAOHONG HUANG[1], CHENG XU[1], (Member, IEEE), PENGFEI WANG[2], AND HONGZHE LIU[3]

[1]Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Smart City Innovation Center, Beijing Shougang Automation & Information Technology Co., Ltd., Beijing 100041, China
[3]Beijing Key Laboratory of Information Service Engineering, Beijing Union University, Beijing 100101, China

Corresponding author: Xiaohong Huang (huangxh@bupt.edu.cn)

This work was supported in part by Joint Funds of National Natural Science Foundation of China and Xinjiang under Grant U1603261, in part by the State Key Program of National Natural Science Foundation of China under Grant 91420202, and in part by the Project of High-level Teachers in Beijing Municipal Universities in the period of the 13th five-year plan under Grant IDHT20170511.

ABSTRACT The Internet of Energy (IoE) provides an effective networking technology for distributed green energy, which allows the connection of energy anywhere at any time. As an important part of the IoE, electric vehicles (EVs), and charging pile management are of great significance to the development of the IoE industry. Previous work has mainly focused on network performance optimization for its management, and few studies have considered the security of the management between EVs and charging piles. Therefore, this paper proposes a decentralized security model based on the lightning network and smart contract in the blockchain ecosystem; this proposed model is called the lightning network and smart contract (LNSC). The overall model involves registration, scheduling, authentication, and charging phases. The new proposed security model can be easily integrated with current scheduling mechanisms to enhance the security of trading between EVs and charging piles. Experimental results according to a realistic infrastructure are presented in this paper. These experimental results demonstrate that our scheme can effectively enhance vehicle security. Different performances of LNSC-based scheduling strategies are also presented.

INDEX TERMS Blockchain, smart contract, vehicle charging, mutual authentication, Internet of Energy.

I. INTRODUCTION

The Internet of energy (IoE) provides an innovative concept for power distribution, energy storage, grid monitoring and communications that will be implemented in future green cities [1]. As a mobile distributed energy storage facility, electric vehicles (EVs) are one of the important components of the IoE. With less air pollution, EVs are gaining widespread adoption and have been deployed in many countries [2], [3].

Recently, both industrial and academic communities have begun to investigate EVs. With the increasing number of EVs, a dense and widespread charging infrastructure will be required. Some work aims to study the deployment of charging stations to determine the optimal setting of charging stations [4]–[6]. Other studies aim to examine scheduling strategies to reduce the resources involved with EVs, such as the time and money spent on charging stations [7]–[9]. However, few works address security problems that could seriously influence the use of electric vehicles.

A blockchain is an open, distributed peer-to-peer data storage mechanism that is designed to efficiently record transactions between two parties in a verifiable and permanent way [10]. Some works try to connect EVs and blockchain technology. In [11], blockchains associated with smart contracts are included in the app development to determine the booking transactions between EVs and charging stations without using a third party. In [12], blockchain technology is used to build a privacy-preserving selection of charging stations. The lightning network and smart contracts are further advances in blockchain technology and have drawn much attention. In [13], a new economic mode for charging pile (CP) sharing is proposed based on the lightning network and smart contracts. However, no detailed design is given in this paper.

In this paper, we propose a novel decentralized security model called the Lightning Network and Smart Contract (LNSC)-based security model to protect transactions between

EVs and charging stations. The main contributions of this paper are three-fold as follows:

1) To the best of our knowledge, this is the first work to investigate authentication mechanisms for EVs and charging management that leverage the lightning network and smart contract technology.

2) A security model is proposed to include registration, scheduling, authentication and charging phases for EV charging management.

3) The security model is evaluated using real EV traffic.

The experimental results show that the LNSC can effectively enhance the security performance of EV charging.

The rest of this paper is structured as follows. Section II introduces related work. Section III introduces the structure of the blockchain ecosystem and security goals. Section IV details the proposed security model. Section V shows the security evaluation. Section VI evaluates the proposed security model integrated with various scheduling algorithms using real EV traffic. Section VII concludes the paper with a summary.

II. RELATED WORK

This section discusses the existing, related work in the management of EV charging issues and the state-of-the-art blockchains.

A. MANAGEMENT OF EV CHARGING

With the increasing number of EVs, the daily charging behavior will inevitably affect the smart grid system. Reasonable management of EVs and charging stations can improve the stability of the smart grid's properties, maintain the system's energy balance, and so on. The management of EV charging has become a key topic in current research on electric vehicles.

In [14], a decentralized control strategy is proposed to reduce the price of recharging. In [15], a dynamic programming formulation is proposed to minimize the long-run average costs through plug-in (hybrid) electric vehicles (PHEVs) scheduling by giving priority to vehicles with less laxity and longer remaining processing times. Considering that the waiting time can be a non-negligible portion of the total work hours, several mechanisms are proposed to reduce the EV driver's wait time at charging stations [**?**], [9], [16]. In [17], a real-time charging station recommendation system for electric vehicle taxis using large-scale GPS data mining is proposed, which provides suggestions for EV taxi drivers and allows them to make their own choices. To avoid the high complexity of solving the dynamic programming problem, a model predictive control (MPC)-based algorithm with computational complexity $O(T^3)$ is proposed in [18], in which T is the sum number of time stages. Security is one of the important aspects in the IoE. However, few works have addressed the secure management of EV charging.

B. BLOCKCHAIN-BASED MANAGEMENT

Blockchains [19], as a distributed, immutable technology, are gaining an increased adaption in many fields, including finance, stock markets, voting, smart contracts, and energy generation and distribution.

The basic processing unit of blockchain technology is the data block. It stores all transaction data and related verification information within a certain time period. Blockchain data are organized into a specific data structure in the form of the chain according to the time sequence. Blockchain uses the SHA 256 algorithm and Merkle tree to implement a simple, efficient, fast and safe storage data management system [20].

Further advances in blockchain technology are the lightning network and smart contracts. The lightning network is a proposed solution to the bitcoin scalability problem [21]. In the blockchain, the consensus calculation and data storage borne by blockchain are mainly from small transactions. The idea of the lightning network is the establishment of a trading management system, but it does not belong to the blockchain system. Both counterparts in the executive system will store and manage the deposit, which allows the small trading information management outside of the blockchain system [22]. In this way, the lightning network has greatly improved the performance of the blockchain system.

Smart contracts were proposed in the prolific cross-field [23]. The smart contract is a set of commitments defined in digital form, and it includes agreements that contract participants can execute. Smart contracts are mostly used for general purpose computations that take place in a blockchain or distributed ledger. The programmable nature of the smart contract not only enables it to be built into the blockchain transaction data but also can be used by consensus to ensure the reliable execution of the contract [24].

Some work aims to connect EV charging management and blockchains. In [11], blockchains associated with smart contracts are included in the app development to determine the booking transactions between EVs and charging stations without using a third party. In [12], blockchain technology is used to build a privacy-preserving selection of charging stations. Based on blockchains, a protocol is proposed to find an optimum charging station that gives public bidding as a response to a query. The customer's geographic position is not revealed during protocol execution, which will in turn protect privacy. In [25], a secure energy trading system is proposed in the Industrial Internet of Things (IIoT) to support fast and frequent energy trading. An optimal pricing strategy using the Stackelberg game is also proposed.

Different from the above mechanisms, this paper aims to study the security model for EV charging management based on the blockchain ecosystem that leverages the lightning network and smart contract technology, which has not yet been addressed in existing works.

III. BLOCKCHAIN ECOSYSTEM MODEL

In this section, the system model for the blockchain ecosystem using the lightning network and smart contracts is presented. The security goal of EV charging management is also defined.

A. SYSTEM MODEL

As addressed previously, this paper aims to investigate the security model for EV charging management based on the blockchain that leverages the lightning network and smart contract technology. The blockchain ecosystem model is shown in Figure 1.

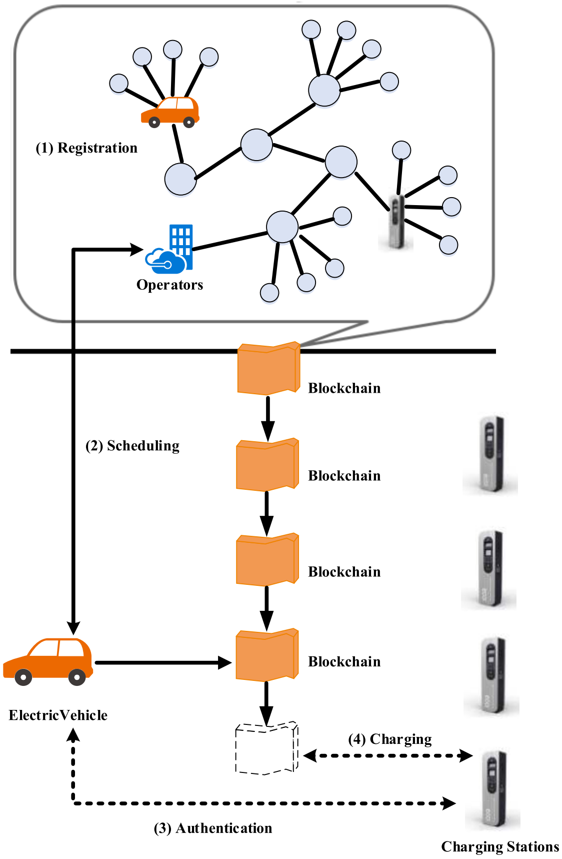

FIGURE 1. The blockchain ecosystem model for electric vehicle and charging pile management.

As shown in Figure 1, in the LNSC scheme, there are four phases in the security model, including the registration phase, scheduling phase, authentication phase and charging phase.

In the first phase, the lightning network is established. The lightning network makes the blockchain network system a trusted third-party to guarantee both parties. It ensures the safety of the funds and payment for the operation. Electric vehicles, charging piles and operators are registered in the lightning network system.

In the second phase, various schedules can be made according to the policies of the carriers and the demands of EV drivers.

In the third phase, EVs and charging piles use elliptic curve cryptography (ECC) to calculate hash functions, which are safe and cannot be calculated against the keys. The mutual authentication between EVs and charging piles validates the signature. If it is valid and matches the identity, the charging requests are accepted.

In the fourth phase, the electric car completes charging, and the charging pile records the transaction's information.

B. SECURITY GOALS

The proposed security model based on the blockchain ecosystem aims to achieve five target security goals [26], [27].

1) KNOWN-KEY SECURITY

Because the shared key is contained in each of the participants using a random number generator to generate short private key, each generated agreement key is unique. Even if the previous key is leaked, the attacker will not get the current key [28].

2) PERFECT FORWARD SECRECY

If a participant or a multi-party participant leaks the private key that was used for long time, it will not affect the shared key that was previously generated. It is the perfect forward to confidentiality [29], [30].

3) KEY CONTROL PROPERTY

Since the shared secret key is generated by the participants of all parties, no one can pre-control the selected value of the shared key for the negotiation [31].

4) RESIST KEY ATTACK

The LNSC should be able to resist the following attack. If the private key of an electric vehicle that has been used for long time leaks, the attacker can impersonate this electric vehicle to deceive others. However, it cannot pretend to be other electric vehicles to cheat this vehicle's user [32], [33].

5) KEY SHARING

Any user participating in the agreement cannot share a key in a situation that other users are not aware of it [34].

IV. PROPOSED SCHEME: LNSC

The notations of LNSC are defined in Table 1.

The initial parameters are as follows. E is the elliptic curve defined in the finite domain $G(q)$. $E(G(q))$ represents the number of points on the elliptic curve that satisfy the equation $a \in Z_n^*$. P is the base of an order of n for the elliptic curve E. G_1 is a cyclic additive group that is generated by $P.f : P \rightarrow Z_n^*$ represents the safe one-way function of a discrete point P to Z_n^* on the elliptic curve. H is a hash function, and E_{pw} denotes the approaches for encrypting with the password. T represents the time stamp, and $sig_i(m)$ represents the user's signature. S is the sole server in the protocol, which is the shared password of the vehicle user and the server. Only the user and the server know S. Then, six secure hash functions are chosen as follows: H_0: $G \rightarrow Z_q^*$, H_1: $\{0, 1\}^* \times G \rightarrow Z_q^*$,

TABLE 1. Definitions of the scheme notations.

Notation	Definition
p, q	Large prime numbers
ID_X	Identity of an entity X
E	Elliptic curve, the basis of order for n
K_i	Shared secret key
C	Commitment
α, m, ζ	User's signature
RID, PID	Real identity and Pseudo-identity
$H\,()$	Cryptographic hash function
M_X	X's authentication information
R_X	Authentication token
‖	Concatenation operation
$\oplus$	XOR operation
SK	Session key

H2: $G \times G \times G \rightarrow Z_q^*$, H3: $\{0, 1\}^* \times \{0, 1\}^* \times G \times \{0, 1\}^* \rightarrow Z_q^*$, H4: $G \times G \times \{0, 1\}^* \rightarrow Z_q^*$ and H5: $\{0, 1\}^* \times \{0, 1\}^* \times G \rightarrow Z_q^*$.

The detailed sequence of the proposed security scheme is shown in Figure 2, including the following four steps: registration, scheduling, authentication and charging.

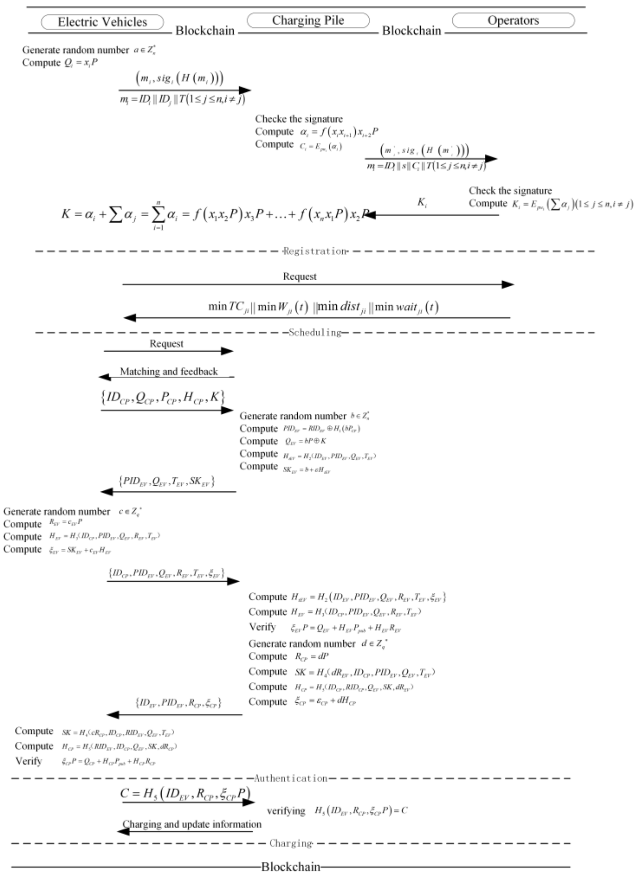
Electric Vehicles
Blockchain
Charging Pile
Blockchain
Operators
Generate random number $a \in Z_n^*$
Compute $Q_i = x_i P$
$(m_i, sig_i(H(m_i)))$
$m_i = ID_i \| ID_j \| T(1 \le j \le n, i \ne j)$
Checke the signature
Compute $\alpha_i = f(x_i x_{i+1}) x_{i+2} P$
Compute $C_i = E_{pw_i}(\alpha_i)$
$(m_i', sig_i(H(m_i')))$
$m_i = ID_i \| s \| C_i \| T(1 \le j \le n, i \ne j)$
Check the signature
Compute $K_i = E_{pw_i}(\sum \alpha_j)(1 \le j \le n, i \ne j)$
K_i
$K = \alpha_i + \sum \alpha_j = \sum_{i=1}^{n} \alpha_i = f(x_1 x_2 P) x_3 P + \ldots + f(x_n x_1 P) x_2 P$
Registration
Request
$\min TC_{ji} \| \min W_{ji}(t) \| \min dist_{ji} \| \min wait_{ji}(t)$
Scheduling
Request
Matching and feedback
$\{ID_{CP}, Q_{CP}, P_{CP}, H_{CP}, K\}$
Generate random number $b \in Z_n^*$
Compute $PID_{EV} = RID_{EV} \oplus H_1(bP_{CP})$
Compute $Q_{EV} = bP \oplus K$
Compute $H_{sEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$
Compute $SK_{EV} = b + \varepsilon H_{sEV}$
$\{PID_{EV}, Q_{EV}, T_{EV}, SK_{EV}\}$
Generate random number $c \in Z_q^*$
Compute $R_{EV} = c_{EV} P$
Compute $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$
Compute $\xi_{EV} = SK_{EV} + c_{EV} H_{EV}$
$\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$
Compute $H_{sEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$
Compute $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$
Verify $\xi_{EV} P = Q_{EV} + H_{EV} P_{pub} + H_{EV} R_{EV}$
Generate random number $d \in Z_q^*$
Compute $R_{CP} = dP$
Compute $SK = H_4(dR_{EV}, ID_{CP}, PID_{EV}, Q_{EV}, T_{EV})$
Compute $H_{CP} = H_5(ID_{CP}, RID_{CP}, Q_{EV}, SK, dR_{EV})$
Compute $\xi_{CP} = \varepsilon_{CP} + dH_{CP}$
$\{ID_{EV}, PID_{EV}, R_{CP}, \xi_{CP}\}$
Compute $SK = H_4(cR_{CP}, ID_{CP}, RID_{EV}, Q_{EV}, T_{EV})$
Compute $H_{CP} = H_5(RID_{EV}, ID_{CP}, Q_{EV}, SK, dR_{CP})$
Verify $\xi_{CP} P = Q_{CP} + H_{CP} P_{pub} + H_{CP} R_{CP}$
Authentication
$C = H_5(ID_{EV}, R_{CP}, \xi_{CP} P)$
verifying $H_5(ID_{EV}, R_{CP}, \xi_{CP} P) = C$
Charging and update information
Charging
Blockchain

FIGURE 2. The detailed sequence of proposed LNSC scheme.

A. REGISTRATION PHASE

The components involved in EV charging management include electric vehicles, charging piles and operators. They are required to register in the open bitcoin blockchain system. In the LNSC, the lightning network transaction management system adopts the mainstream cloud platform based on the Internet environment's architecture. The following is the registration process.

Step 1: EVs $\{V_1, V_2, \ldots, V_n\}$ randomly select $x \in Z_n^*$ and compute $Q_i = x_i P$. Then, they broadcast $(m_i, sig_i(H(m_i)))$ and $m_i = ID_i||ID_j||T\ (1 \le j \le n, i \ne j)$. EVs place a request in the blockchain.

Step 2: Charging piles first check the signature and then calculate the amount of its own signature $\alpha_i = f(x_i x_{i+1}) x_{i+2} P$. Then, $C_i = E_{pw_i}(\alpha_i)$ is calculated. After that, charging piles send both $\left(m_i', sig_i\left(H\left(m_i'\right)\right)\right)$ and $m_i = ID_i||s||C_i||T\ (1 \le j \le n, i \ne j)$ to Operator O in the blockchain.

Step 3: Operator O validates the signature and reuses the pw_i that each user shares with the decryption signature α_i. Then, $K_i = E_{pw_i}\left(\sum \alpha_j\right) (1 \le j \le n, i \ne j)$ is computed and K_i is broadcasted in the blockchain.

Step 4: Each participant receives K_i, and the session key $K = \alpha_i + \sum \alpha_j = \sum_{i=1}^{n} \alpha_i = f(x_1 x_2 P) x_3 P + \ldots + f(x_n x_1 P) x_2 P$ is calculated. Once a request is in the blockchain, it is visible to all charging stations.

B. SCHEDULING PHASE

In the LNSC scheme, four types of scheduling strategies, i.e., the shortest path scheduling, minimum time cost scheduling, minimum comprehensive cost scheduling, and minimum waiting time scheduling, are adopted to schedule the charging piles.

1) SHORTEST PATH-BASED SCHEDULING

The distance of the electric vehicle to each charging pile is calculated, based on which, the charging pile i with the minimum distance value min $dist_{ji}$ is selected. After that, the ending time of charging $endt_i$ is updated.

2) TIME COST-BASED SCHEDULING

The time costs TC_{ji} for the electric vehicle to arrive at each charging pile are calculated, based on which, the charging pile i with the minimum time cost min TC_{ji} is selected. After that, the ending time of charging $endt_i$ is updated.

3) COMPREHENSIVE COST-BASED SCHEDULING

The comprehensive costs consist of consumption costs and time costs. The $W_{ji}(t)$ of charging the electric vehicle at each charging pile is calculated, based on which the charging pile i with min $W_{ji}(t)$ is selected. After that, the ending time of charging $endt_i$ is updated.

4) WAITING TIME-BASED SCHEDULING

The waiting times $wait_{ji}(t)$ of the charging electric vehicle at each charging pile are calculated, and then the charging pile i corresponding to the minimum waiting time min $wait_{ji}(t)$ is selected. After that, the ending time of charging $endt_i$ is updated.

C. AUTHENTICATION PHASE

In the LNSC scheme, the EV and charging pile conduct a point-to-point transaction, and mutual authentication is used to enhance trading flexibility. After the EV receives the scheduling recommendation given by the operator, a two-way authorization is made between the EV and the selected charging pile. When the EV arrives at the charging pile location, the authentication phase will be conducted. The process of mutual authentication is as follows.

Step 1: The vehicle sends its identity ID_{EV} to the charging pile. The selected charging pile gathers the information from the blockchain that matches and returns the charge request to the EV.

Step 2: The electric vehicle sends $\{ID_{CP}, Q_{CP}, P_{CP}, H_{CP}, K\}$ to the charging pile.

Step 3: The charging pile chooses a random number $b \in Z_q^*$ with the current timestamp T_i. Then, it computes the values of $PID_{EV} = RID_{EV} \oplus H_1(bP_{CP})$, $Q_{EV} = bP \oplus K$, $H_{tEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$ and $SK_{EV} = b + \varepsilon H_{tEV}$. After that, the message $\{PID_{EV}, Q_{EV}, T_{EV}, SK_{EV}\}$ is sent to EV.

Step 4: The EV chooses a random number $c \in Z_q^*$, and computes $R_{EV} = c_{EV}P$, $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$, and $\xi_{EV} = SK_{EV} + c_{EV}H_{EV}$. Then, the EV sends message $\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$ to the charging pile using the secure channel.

Step 5: The CP receives the request message of $\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$, and then calculates $H_{tEV} = H_2(ID_{EV}, PID_{EV}, Q_{EV}, T_{EV})$ and $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$. Based on $\xi_{EV}P = Q_{EV} + H_{EV}P_{pub} + H_{EV}R_{EV}$, the signature received is verified. If the verification fails, the charging pile terminates the session. Otherwise, the charging pile calculates the true identity of the EV. The charging pile chooses a random number $d \in Z_q^*$, and then 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 $\xi_{CP} = \varepsilon_{CP} + dH_{CP}$. Then, the charging pile sends the message $\{ID_{EV}, PID_{EV}, R_{CP}, \xi_{CP}\}$ to the EV.

Step 6: The EV receives $\{ID_{EV}, PID_{EV}, R_{CP}, \xi_{CP}\}$. Then, it computes the value of $SK = H_4(cR_{CP}, ID_{CP}, RID_{EV}, Q_{EV}, T_{EV})$ and $H_{CP} = H_5(RID_{EV}, ID_{CP}, Q_{EV}, SK, dR_{CP})$. Based on the equation $\xi_{CP}P = Q_{CP} + H_{CP}P_{pub} + H_{CP}R_{CP}$, the received signature is verified. If the verification passes, the mutual authentication is finished. Otherwise, the EV terminates the session. After authentication, a secret session key SK is generated that can be used to encrypt messages to achieve secure communications.

Since it is a point-to-point transaction and uses mutual authentication, the trading parties will not affect the market.

D. CHANGING PHASE

In this section, the electric vehicle completes charging and updates the transaction's information. This commitment is written in the blockchain.

Step 1: The EV computes a hidden and computationally binding commitment $C = H_5(ID_{EV}, R_{CP}, \xi_{CP}P)$. It includes the identity ID of the EV, the random parameter R_{CP} computed by charging pile, and the signature $\xi_{CP}P$.

Step 2: The charging pile checks the commitment by verifying $H_5(ID_{EV}, R_{CP}, \xi_{CP}P) = C$, and then determines whether the current time matches the initially proposed timeframe of the EV.

Step 3: Charging commences between the EV and the chosen charging pile. No information is released in the blockchain and no third-party information is publicly available in the blockchain.

V. SECURITY EVALUATION

In this section, the security of the LNSC scheme is analyzed. The Burrows–Abadi–Needham (BAN) logic is used to confirm the security mutual authentication between the electric vehicle and the charging pile. In addition, the security goals were analyzed to assess whether the proposed scheme is secure and efficiently enhances vehicle security.

A. LOGIC PROOF OF AUTHENTICATION

In this section, the formal analysis method is used to prove the security protocol. Logic proof analysis is the most widely used formal method. It plays an important role in verifying security protocols, especially the analysis of the authentication protocol. The BAN logic is used to confirm the secure mutual authentication between the electric vehicle and charging pile.

The logical symbols and inference rules of the BAN logic are described as follows.

(1) *A, B*: subjects, that is, the principal participants in the protocol.
(2) X: message.
(3) K: secret key.
(4) $\{X\}_K$: message X is encrypted with K.
(5) $A| \equiv B$: A believes B.
(6) $A \lhd X$: A has received message X.
(7) $A| \sim X$: A said X.
(8) $B \Rightarrow X$: B has the jurisdiction to X.
(9) *#(X)*: X is fresh.
(10) $A \overset{K}{\longleftrightarrow} B$: K is the common preshared key of A and B.

In the following, based on the BAN logic model, we will express that the mutual authentication and key agreement between the EV and the charging pile can be correctly realized. The proof process is as follows:

1) PROTOCOL IDEALIZATION

To facilitate the formal analysis, when performing the BAN logic analysis, the first step is to convert every step of the authentication into the idealized form.

$$m_1 : EV : \langle PID_{EV}, Q_{EV} \rangle_{SK_{EV}}$$

$$m_2 : EV \to CP : \langle ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, K \rangle_{SK_{EV}}$$

$$m_3 : CP \to EV : \langle PID_{EV}, ID_{CP}, R_{CP}, K \rangle_{SK_{CP}}$$

$$m_4 : EV : \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle_{S_{EV}}$$

$$m_5 : EV \to CP : \left\langle EV \overset{K}{\longleftrightarrow} CP \right\rangle_{SK}$$

$$m_6 : CP \to EV : \left\langle CP \overset{K}{\longleftrightarrow} EV \right\rangle_{SK}$$

2) INITIAL ASSUMPTION

The initial assumption is the important guarantee that the LNSC analysis will be successfully conducted. Its assumption includes the key that is initially shared, the trusted equipment in some situations, and the equipment that generates a new value. The initial assumptions for the proposed agreement are as follows.

$$A1 : EV \overset{H(ID_{EV}\|T)}{\longleftrightarrow} CP$$

$$A2 : EV \left| \xrightarrow{P_{CP}} CP \right.$$

$$A3 : CP \overset{H(ID_{CP}\|T)}{\longleftrightarrow} EV$$

$$A4 : EV \mid\equiv \#EV \Rightarrow EV \overset{P}{\longleftrightarrow} CP$$

$$A5 : CP \left| \xrightarrow{P_{EV}} EV \right.$$

$$A6 : EV \mid\equiv EV \mid\Rightarrow P$$

$$A7 : EV \mid\equiv CP \mid\Rightarrow Q$$

3) PROTOCOL GOAL

The ultimate goal of the LNSC scheme is to realize the mutual authentication between the EV and charging pile and establish a shared session key. The expressions of the objectives are presented by the BAN logic as follows.

$$Goal1 : EV \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$$

$$Goal2 : EV \mid\equiv CP \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$$

$$Goal3 : CP \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$$

$$Goal4 : CP \mid\equiv EV \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$$

4) PROTOCOL ANNOTATIONS AND TARGET DERIVATION

Based on m1, the following statement can be obtained.

Statement 1: $EV \lhd \langle PID_{EV}, Q_{EV} \rangle_{SK_{EV}}$

Based on Statement 1 and A1, by the message-meaning rule,

Statement 2: $EV \mid\equiv EV \mid\sim \langle PID_{EV}, Q_{EV} \rangle$

Based on Statement 2, by the fresh value validation and freshness verification rules,

Statement 3: $EV \mid\equiv \langle ID_{EV} \rangle$

Based on m2,

Statement 4: $EV \lhd \langle ID_{EV} \rangle_{SK}$

Based on Statement 4 and A2, by the message-meaning rule,

Statement 5: $EV \mid\equiv EV \mid\sim \langle P \rangle$

Based on Statement 5, by the freshness verification rule,

Statement 6: $EV \mid\equiv \langle P \rangle$

Based on m3,

Statement 7: $EV \lhd \left\langle ID_{CP}, EV \overset{P}{\longleftrightarrow} CP \right\rangle_{H(ID_{EV}\|T)}$

Based on Statement 7 and A3, by the message-meaning rule,

Statement 8: $EV \mid\equiv EV \mid\sim \left\langle EV \overset{H(ID_{EV}\|T)}{\longleftrightarrow} CP \right\rangle$

Based on Statement 8, by the fresh value validation and freshness verification rules,

Statement 9: $EV \mid\equiv \left\langle EV \overset{P}{\longleftrightarrow} CP \right\rangle$

Based on Statement 9 and A4, by the control rule,

Statement 10: $EV \mid\equiv \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle$ (Goal 1)

Based on m4,

Statement 11: $CP \lhd \left\langle EV \overset{Q}{\longleftrightarrow} CP \right\rangle_{S_{EV}}$

Based on Statement 11 and A5, by the message-meaning rule,

Statement 12: $CP \mid\equiv EV \mid\sim \left\langle EV \overset{Q}{\longleftrightarrow} CP \right\rangle$

Based on Statement 12 and A6, the fresh value validation and freshness verification rules,

Statement 13: $CP \mid\equiv EV \mid\equiv \left\langle EV \overset{Q}{\longleftrightarrow} CP \right\rangle$

Based on Statement 12 and A7, by the control rule,

Statement 14: $EV \mid\equiv CP \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$ (Goal 2)

Based on m5,

Statement 15: $EV \lhd \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle_{SK}$

Based on Statement 15, by the message-meaning rule,

Statement 16: $EV \mid\equiv CP \mid\sim \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle$

Based on Statement 16, by the fresh value validation and freshness verification rules,

Statement 17: $EV \mid\equiv CP \mid\equiv \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle$

Based on Statement 17,

Statement 18: $CP \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$ (Goal 3)

Based on m6,

Statement 19: $CP \lhd \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle_{SK}$

Based on Statement 19, by the message-meaning rule,

Statement 20: $CP \mid\equiv EV \mid\sim \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle$

Based on Statement 20, by the fresh value validation and freshness verification rules,

Statement 21: $CP \mid\equiv EV \mid\equiv \left\langle EV \overset{SK}{\longleftrightarrow} CP \right\rangle$

Based on Statement 21,

Statement 22: $CP \mid\equiv EV \mid\equiv EV \overset{SK}{\longleftrightarrow} CP$ (Goal 4)

By the logical presentation and derivation, we can obtain Goals 1–4, which show that the LNSC scheme can realize the mutual authentication and session key agreement between the EV and charging pile.

B. SECURITY ANALYSIS

Proposition 1. The LNSC scheme can realize known-key security.

Proof: A secure and trusted transaction of the charging pile sharing support the EV and the charging pile mutual authentication. No efficient algorithm can solve the elliptic curve discrete logarithm problem (ECDLP) with less than exponential time. The LNSC uses elliptic curve encryption to calculate the hash functions. The smart contract based on the hash key for known-key security verification includes the following steps:

(1) The charging pile generates $R_{EV} = c_{EV}P$ and records the transmission using the P2P network. The lightning network sets up the charging quantity of the agreement, and the hash $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$ is sent to the EV. Then, the hash key $\{ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV}, \xi_{EV}\}$ is kept.

(2) The payment channels network is established. The contract stipulates the amount of the transaction, the transfer terms, and sets the trigger condition to obtain the correct key $H_{EV} = H_3(ID_{CP}, PID_{EV}, Q_{EV}, R_{EV}, T_{EV})$.

(3) The contract is executed to verify that the signature received is valid by $\xi_{EV}P = Q_{EV} + H_{EV}P_{pub} + H_{EV}R_{EV}$. If the verification fails, the charging pile terminates the session.

(4) The contract is checked to verify that the received signature is valid using $\xi_{CP}P = Q_{CP} + H_{CP}P_{pub} + H_{CP}R_{CP}$. If verification fails, the electric vehicle terminates the session.

Thus, the LNSC scheme can realize known-key security.

Proposition 2: The LNSC scheme can realize perfect forward secrecy.

Proof: The corresponding operational permissions of all principals on a resource are recorded on the blockchain and are publicly visible to all subjects. If a resource owner maliciously rejects a request for access to a given condition, it can be publicly audited and punished accordingly. Furthermore, the application of the smart contract function through the blockchain can implement the self-enforcement of the access request.

Proposition 3: The LNSC scheme can realize the key control property

Proof: Every time an agreement starts, the temporary private keys of the electric vehicles, charging piles and operators will be different. The LNSC utilizes signature $\xi_{CP}P = Q_{CP} + H_{CP}P_{pub} + H_{CP}R_{CP}$ and $\xi_{EV}P = Q_{EV} + H_{EV}P_{pub} + H_{EV}R_{EV}$ authentication. Thus, in the LNSC, the key is not controllable.

Proposition 4: The LNSC scheme can resist key attack

Proof: In the LNSC scheme, no single access control node is available. The nodes are scattered in various resource owner permissions so that the DDOS attacker loses a single target. The access control policy is kept in blockchain so that it can be kept on all nodes and maintained by the consensus of the blockchain mechanism. It is impossible for anyone to tamper with the transactions. On the basis of the secure elliptic curve, the difficulty of the discrete logarithm in the elliptic curve can effectively ensure the security of the key parameters $SK_{EV} = b + \varepsilon H_{tEV}$ and $\xi_{EV} = SK_{EV} + c_{EV}H_{EV}$ in the communication process.

In key agreement authentication, the LNSC provides mutual authentication for electric vehicles and charging piles. It uses elliptic curve encryption to calculate the hash functions. It can resist key leakage attacks. Thus, it can resist the security features of key attack and tamper-proof. Besides, the attacker doesn't know the private keys and cannot compute computational discrete logarithm (CDL) problem. Thus, it can resist the security features of key attack, replay attacks, impersonation attacks, modification attacks and man-in-the-middle attacks and tamper-proof.

Proposition 5: The LNSC scheme can realize key sharing security.

Proof: In the LNSC scheme, the agreement of the shared secret key is generated by random number $\{a, b, c, d\}$ and $a, b, c, d \in Z_q^*$ from each participant's short private key. The key generated in each agreement is unique. Therefore, the LNSC realizes key sharing security.

VI. PERFORMANCE ANALYSIS

A. EXPERIMENTAL ENVIRONMENT

In this paper, a real test scenario is constructed to evaluate the performance of the proposed security model. The charging operational platform includes a charging management platform for operators and a charging service platform for charging customers. There are 60 charging piles in the network, including 40 direct current (DC) charging piles and 20 alternating current (AC) charging piles. The charging piles are shown in Figure 3.

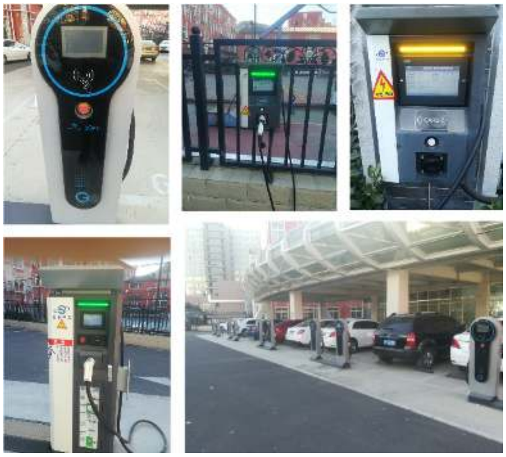

FIGURE 3. Charging station overview, including DC charging piles and AC charging piles.

B. ANALYSIS OF DEALSUCCESSMSG EXECUTION

In Table 2, the results of the DealSuccessMsg execution are shown. The number of nodes in the network is 300, and the time of the execution is one month. As showed in table 2, 1037 total DealSuccessMsgs are signed, among which 1004 are successfully executed for a success rate of approximately 97.78%. The confirmation time for each DealSuccessMsg payment is approximately 16 seconds on average. The main failure reason of a DealSuccessMsg is insufficient funds for the electric vehicles.

C. ANALYSIS OF COMPUTATIONAL COST FOR CRYPTOGRAPHIC OPERATIONS

The experimental hardware is an Intel Core i7-4790 processor with a 3.60-GHz clock frequency and 32G memory.

TABLE 2. The DealSuccessMsg execution.

Time	Authentication Signing	Execute	Failure
7 days	266	258	8
7 days	252	245	7
7 days	272	266	6
7 days	247	245	2
Total	1037	1014	21

TABLE 3. Cryptographic operations list.

	Name	Cryptograph in operations	Execution time (ms)
Bilinear Pairing	A bilinear pairing operation	T_{bp}	6.7263
	A scale multiplication operation	T_{bm}	2.1183
	A small factor multiplication operation	T_{bsm}	0.5166
	A point addition operation	T_{ba}	0.2201
Elliptic Curve Cryptogr aphy	A scale multiplication operation	T_{em}	0.9562
	A small-scale multiplication operation	T_{esm}	0.1387
	An exponentiation operation	T_{ex}	0.6238
	A point addition operation	T_{ea}	0.0828
A general hash function operation		T_h	0.0012
A map-to-point operation		T_{mtp}	5.155

The Windows 10 operating system was used. The execution time of the proposed cryptographic operations was calculated using MIRACL [35]. The MIRACL library is a famous cryptographic operations library and has been widely used to implement cryptographic operations in many environments. The computational tool is VS 2010. The execution times of the cryptographic operations are listed in Table 3. It defines some of the execution times results to further the analysis of the computational overhead. As shown in Table 3, the cryptograph execution times are calculated separately for the bilinear pairing and elliptic curve cryptography.

TABLE 4. Computational costs of different schemes.

Scheme	EV	CP
Lai's AMA[30]	$7T_{bm}+T_{ba}+T_{mtp}$ ≈ 20.7386 ms	$2T_{bp}+5T_{bm}+T_{ba}+T_{mtp}$ ≈ 29.4192 ms
Qiu's EPH[32]	$2T_{esm}+3T_{ea}+8T_h$ ≈ 0.5354 ms	$2T_{em}+4T_{ea}+5T_h$ ≈ 2.2508 ms
LNSC	$T_{esm}+2T_{ea}+3T_h$ ≈ 0.3079 ms	$2T_{em}+2T_{ea}+6T_h$ ≈ 2.0852 ms

The computational costs of the LNSC will be compared with those of other schemes [30], [32]. Table 4 demonstrates the major benefits of the proposed LNSC scheme in mutual authentication and key agreement. From table 4, we find that the LNSC works better in terms of computational costs.

D. ANALYSIS OF PERFORMANCE OF SCHEDULING STRATEGIES

In this subsection, the performances of various scheduling strategies are evaluated in terms of consumption costs and time costs. The results can lead to recommendations for the operators to select the appropriate scheduling strategies. The number of vehicles introduced per hour is displayed in Table 5.

TABLE 5. The number of electric vehicles introduced at different times.

Time quantum	Number of vehicles (quantity/h)
00:00-04:00	30
04:00-08:00	20
08:00-12:00	40
12:00-16:00	30
16:00-20:00	20
20:00-24:00	30

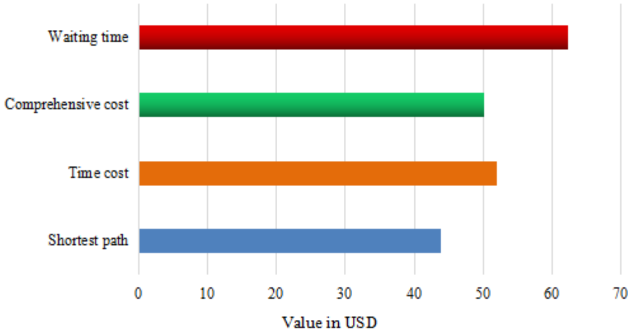

FIGURE 4. The performance of consumption costs for each electric vehicle in one month using different scheduling methods.

1) CONSUMPTION COSTS

Figure 4 shows consumption costs for each electric vehicle charged at 2 p.m. It shows that the total consumption costs in one month for four scheduling methods are $ 43.95, $ 51.96, $ 50.08, and $ 62.31.

From the figure, it is easy to find that the shortest path-based scheduling method obtains the best performance in terms of consumption costs. It is because the more distance the EV drives to charging pile, the more costs that will be paid. For time cost-based scheduling and waiting time cost-based scheduling, to save time, the charging pile with the shortest distance will be recommended to the EVs. Comprehensive cost-based scheduling aims to achieve a balance between consumption costs and time costs. Hence, it is able to work better than time cost-based scheduling and waiting time cost-based scheduling.

Figure 5 shows the charging cost for each electric vehicle when the time is 2 p.m. It shows that except for the waiting time mode, the user consumption cost fluctuation is stable with the changes of vehicles. In addition, the comprehensive cost mode and shortest path mode that both do not consider the time are the best selections.

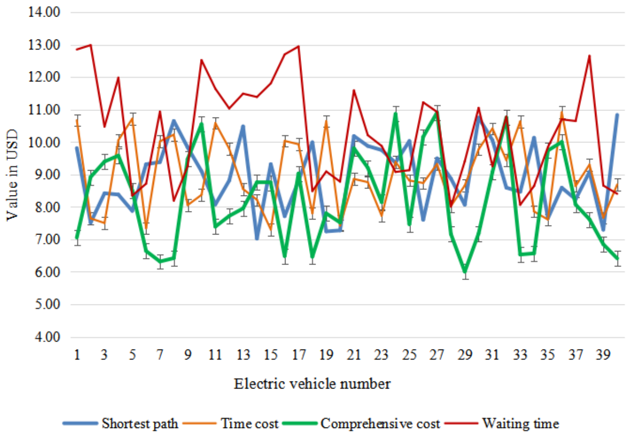

FIGURE 5. The performance of consumption cost for each electric vehicle when the time is 2 p.m using different scheduling methods.

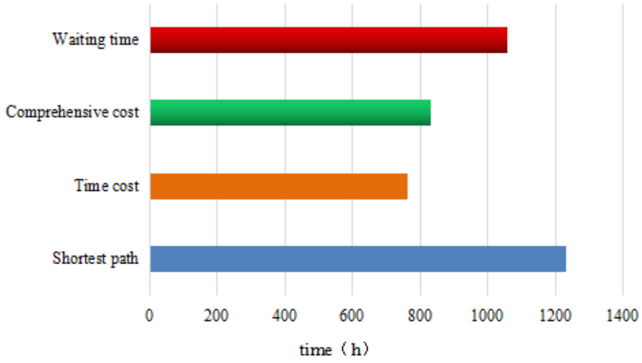

FIGURE 6. The performance of time costs for each electric vehicle in one month using different scheduling methods.

2) TIME COST

The performances of time costs for the four scheduling strategies are shown in Figure 6, which shows that the average times for EV charging in one year are respectively 1233.28 h, 762.49 h, 831.68 h, and 1056.33 h.

From the figure, we can find that the time cost-based scheduling works best in terms of time costs. It is obvious because the time costs are the main concern for this scheduling algorithm. Furthermore, the shortest path-based scheduling works worst in this case. It is because the shortest path-based scheduling only considers the distance to the charging pile. However, in heavy traffic congestion, more time will be taken by the EVs in waiting for charging. Therefore, the time costs are the highest. For waiting time-based scheduling, it does not include the distance to the charging pile, and thus, it will take a longer time on the way. It is interesting to find that comprehensive cost-based scheduling still ranks second due to the good balance of consumption costs and time costs it achieves.

Figure 7 shows the time costs of charging for each electric vehicle when the time is 2 p.m. It shows that the shortest path based and waiting time-based scheduling have the bigger time costs. In addition, the comprehensive cost mode and time cost mode that do not consider consumption are the best selections.

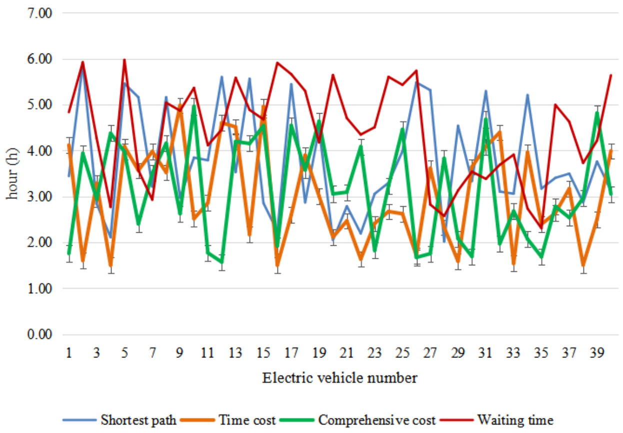

FIGURE 7. The performance of time cost for each electric vehicle when the time is 2 p.m using different scheduling methods.

VII. CONCLUSION

In this paper, a decentralized security model for EV charging management in the IoE, called the LNSC, has been proposed. This model leverages the lightning network and smart contracts in a blockchain ecosystem. The logic correctness of the LNSC has been proven. By the security analysis, the LNSC is able to meet the expected security goals. The performance of the LNSC has been evaluated in terms of computation costs, which shows that the LNSC is able to achieve lower computation costs than other existing solutions. Meanwhile, experiments have been done using a real network scenario to evaluate the performance of the LNSC. The results show that a 97.78% success rate can be achieved for the method, and comprehensive cost-based scheduling is able to achieve a good balance of consumption costs and time costs, which can be the recommendations for the operators to select the appropriate scheduling strategies.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and the Editor for providing constructive and generous feedback on this paper.

REFERENCES

[1] K. Wang *et al.*, “A survey on energy Internet: Architecture, approach, and emerging technologies,” *IEEE Syst. J.*, to be published.

[2] V. Cheung. (2016). *South Korea Releases Electric Public Transportation System*. [Online]. Available: http://globalenergyinitiative.org/south-korea-releases-electric-public-transportation-system.html

[3] (2014). *Electric Bus*. [Online]. Available: http://www.transitchicago.com/electricbus/

[4] P. Jochem, C. Brendel, M. Reuter-Oppermann, W. Fichtner, and S. Nickel, “Optimizing the allocation of fast charging infrastructure along the German autobahn,” *J. Bus. Econ.*, vol. 86, no. 5, pp. 513–535, 2016.

[5] M. Gharbaoui, B. Martini, R. Bruno, L. Valcarenghi, M. Conti, and P. Castoldi, “Designing and evaluating activity-based electric vehicle charging in urban areas,” in *Proc. Electr. Vehicle Conf.*, Oct. 2013, pp. 1–5.

[6] J. Jung, J. Y. J. Chow, R. Jayakrishnan, and J. Y. Park, “Stochastic dynamic itinerary interception refueling location problem with queue delay for electric taxi charging stations,” *Transp. Res. C, Emerg. Technol.*, vol. 40, no. 1, pp. 123–142, 2014.

[7] F. Malandrino, C. Casetti, and C. F. Chiasserini, "A holistic view of ITS-enhanced charging markets," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1736–1745, Aug. 2015.

[8] H. Qin and W. Zhang, "Charging scheduling with minimal waiting in a network of electric vehicles and charging stations," in *Proc. 8th Int. Workshop Veh. Ad Hoc Netw. (VANET)*, Las Vegas, NV, USA, Sep. 2011, pp. 51–60.

[9] J. L. Lu, M.-Y. Yeh, Y.-C. Hsu, S.-N. Yang, C.-H. Gan, and M.-S. Chen, "Operating electric taxi fleets: A new dispatching strategy with charging plans," in *Proc. Electr. Vehicle Conf.*, Mar. 2012, pp. 1–8.

[10] M. Iansiti and K. R. Lakhani, *The Truth About Blockchain—Harvard Business Review*. Cambridge, MA, USA: Harvard Univ., 2017.

[11] A. Dubois, A. Wehenkel, R. Fonteneau, F. Olivier, and D. Ernst, "An app-based algorithmic approach for harvesting local and renewable energy using electric vehicles," in *Proc. Int. Conf. Agents Artif. Intell.*, 2017, pp. 322–327.

[12] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 71–79, 2017.

[13] Q. I. Linhai *et al.*, "Shared economy model of charging pile based on block chain ecosystem," *Electr. Power Construction*, vol. 38, no. 9, pp. 1–7, 2017.

[14] L. Gan, U. Topcu, and S. H. Low, "Optimal decentralized protocol for electric vehicle charging," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 940–951, May 2013.

[15] Y. Xu, F. Pan, and L. Tong, "Dynamic scheduling for charging electric vehicles: A priority rule," *IEEE Trans. Autom. Control*, vol. 61, no. 12, pp. 4094–4099, Dec. 2016.

[16] H.-J. Kim, J. Lee, G.-L. Park, M.-J. Kang, and M. Kang, "An efficient scheduling scheme on charging stations for smart transportation," in *Security-Enriched Urban Computing and Smart Grid*. Berlin, Germany: Springer, 2010.

[17] Z. Tian *et al.*, "Real-time charging station recommendation system for electric-vehicle taxis," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 11, pp. 3098–3109, Nov. 2016.

[18] W. Tang and Y. J. A. Zhang, "A model predictive control approach for low-complexity electric vehicle charging scheduling: Optimality and scalability," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1050–1063, Mar. 2016.

[19] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[20] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[21] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," Blockchain, Luxembourg, DRAFT Version 0.5.9.2, 2015. [Online]. Available: http://www.the-blockchain.com/docs/Lightning%20Network%20Whitepaper.pdf

[22] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, 2017.

[23] L. M. Surhone, *Smart Contract*. MT, USA: Betascript, 2010.

[24] H.-T. Wu and G.-J. Horng, "Establishing an intelligent transportation system with a network security mechanism in an Internet of vehicle environment," *IEEE ACCESS*, vol. 5, pp. 19239–19247, 2017.

[25] H. Zhu and X. Hao, "A provable authenticated key agreement protocol with privacy protection using smart card based on chaotic maps," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 1–11, 2015.

[26] A. G. Reddy, A. K. Das, E.-J. Yoon, and K.-Y. Yoo, "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography," *IEEE ACCESS*, vol. 4, pp. 4394–4407, 2016.

[27] C. Lin, J. Zhou, C. Guo, H. Song, G. Wu, and M. S. Obaidat, "TSCA: A temporal-spatial real-time charging scheduling algorithm for on-demand architecture in wireless rechargeable sensor networks," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 211–224, Jan. 2018.

[28] H. Zhu and X. Hao, "An efficient authenticated key agreement protocol based on chaotic maps with privacy protection using smart card," *Nonlinear Dyn.*, vol. 81, nos. 1–2, 2015, pp. 1–11.

[29] H. Arshad and M. Nikooghadam, "Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol," *J. Supercomput.*, vol. 71, no. 8, pp. 3163–3180, 2015.

[30] C. Lai, R. Lu, H. Li, D. Zheng, and X. S. Shen, "Secure machine-type communications in LTE networks," *Wireless Commun. Mobile Comput.*, vol. 16, no. 12, pp. 1495–1509, 2016.

[31] Y. Liu and K. Xue, "An improved secure and efficient password and chaos-based two-party key agreement protocol," *Nonlinear Dyn.*, vol. 84, no. 2, pp. 549–557, 2016.

[32] Y. Qiu, M. Ma, and X. Wang, "A proxy signature-based handover authentication scheme for LTE wireless networks," *J. Netw. Comput. Appl.*, vol. 83, pp. 63–71, Apr. 2017.

[33] T. Zou, S. Lin, Q. Feng, and Y. Chen, "Energy-efficient control with harvesting predictions for solar-powered wireless sensor networks," *Sensors*, vol. 16, no. 1, p. 53, 2016.

[34] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud," *IEEE Trans. Comput.*, vol. 66, no. 5, pp. 891–904, May 2017.

[35] Miracl, London, U.K. (2017). *Miracl Library*. [Online]. Available: http://www.miracl.com

XIAOHONG HUANG received the B.E. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2000, and the Ph.D. degree from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2005. Since 2005, she has been with BUPT, where she is currently an Associate Professor and the Director of Network and Information Center, Institute of Network Technology. She has published over 50 academic papers in the area of WDM optical networks, IP networks, and other related fields. Her current interests include optimization of computer networks, network security, and so on.

CHENG XU (M'17) received the B.E. and M.A.Sc. degrees from the Beijing Key Laboratory of Information Service Engineering, Beijing Union University, China, in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Institute of Network Technology, Beijing University of Posts and Telecommunications, Beijing, China. Since 2012, he has been involved in Intelligent Drive and Internet of Vehicles. He made report in the IEEE International Conferences on High Performance Computing and Communications in 2017. His current research interests include wireless security and vehicular network.

PENGFEI WANG received the B.E. degree and M.A.Sc. degrees from Beijing Union University, Beijing, China, in 2012 and 2015, respectively. In 2015, he joined the Beijing Shougang Automation & Information Technology Co., Ltd., and involved in the smart building project for the 2022 Beijing Winter Olympic Games and Paralympic Games, where he is currently a Smart City Planner with the Smart City Innovation Center. His current research interests include smart building and artificial intelligence.

HONGZHE LIU received the B.E. degree from Chinese Marine University, China, in 1995, and the M.A.Sc. degree from California State University, Los Angeles, CA, USA, in 2000, and the Ph.D. degree from Beijing Jiaotong University, Beijing, China. She is currently a Professor with Beijing Union University, where he is the Vice Director of Beijing Key Laboratory of Information Service Engineering. Her research interests include artificial intelligence and Internet of Things. She is a member of the Chinese Computer Society and the reviewer of the National Natural Fund. She serves as a reviewer for many domestic and foreign periodicals. She is the Vice Secretary General of the Network Application Branch, China Computer User Association.