IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 1, 2020, accepted June 16, 2020, date of publication June 29, 2020, date of current version July 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005400

A Secure and Anonymous Communication Scheme for Charging Information in Vehicle-to-Grid

JINGTANG LUO[1], (Member, IEEE), SHIYING YAO[1], JIAMIN ZHANG[2], WEITING XU[1], YUN HE[2], AND MIN ZHANG[2], (Member, IEEE)

[1]State Grid Sichuan Economic Research Institute, Chengdu 610041, China
[2]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Corresponding author: Jiamin Zhang (zhangjm_ustb@163.com)

This work was supported in part by the State Grid Science and Technology Research Program under Grant B3441520K001, and in part by the National Natural Science Foundation of China under Grant 61941113, Grant 61971033, and Grant 61671057.

ABSTRACT With electric vehicle's charging information, the utilities can increase the efficiency and reliability of Vehicle-to-Grid (V2G) while the electric vehicle consumers can better manage their energy consumption and costs. However, since charging information are commonly transmitted via public network or wireless link, their communications lack trusted third party for identity authentication and key distribution, and are constantly exposed to traffic analysis attacks. In this article, we propose a secure and anonymous communication scheme for delivering charging information in V2G. Different from previous works, the scheme in this article creatively incorporates identity authentication into key distribution without trusted third party, which improves the security of communication in public networks. Moreover, the proposed scheme is more resistant to traffic analysis since it preserves the anonymity of charging information by splitting and forwarding them pseudo-randomly. As the performance analysis reveals, our scheme is able to provide better anonymity without the support of trusted third party, and what's more, it can achieve high cryptography capability as traditional communication schemes do. Therefore, it is more practical in real-world V2G.

INDEX TERMS V2G, data transmission, identity authentication, anonymous transmission.

I. INTRODUCTION

With the development of the logistics industry and the growth of the number of vehicles, the pressure of the road transportation system is increasing explosively [1]. To improve the efficiency and safety of transportation and reduce environmental pollution, intelligent transportation system was emerged [2]. As the main member of the system, electric vehicles (EVs) have gradually become a hotspot of global research. Vehicle-to-Grid (V2G) is a technology that uses on-board batteries of EVs as a distributed energy storage unit to achieve two-way transmission of energy and information between the vehicle and the grid [3]. The core idea is to controllably feedback the residual energy to the grid according to the intelligent charging/discharging strategy. Through combining EVs, communication networks, control systems, and computer processing, V2G can efficiently use the grid's energy, reduce environmental impacts, and facilitate the integration of renewables [4]–[7].

EVs' charging information is one of the most important data for intelligent transportation system to operate stably and efficiently. For instance, they can be used to reduce peak loads, set flexible prices, and improve investment efficiency [8]. However, while EVs' charging information is greatly valuable for the control and management of intelligent transportation system, it also brings security risks and privacy leakage issues to the EV users and the utilities [9]. Specifically, the communication links between EVs and up-stream nodes (e.g., concentrators and central systems [10]) are usually wireless links or public links provided by Internet Service Providers (ISPs), which are potentially vulnerable to various network attacks like identify forgery [11], message tampering [9], or traffic analysis [12]. The forged identity of EVs or central system or tampered charging information can easily mislead the billing system and causes significant economic losses. Charging information may also be analyzed

The associate editor coordinating the review of this manuscript and approving it for publication was Amr Tolba.

to dig out sensitive personal information about consumers, including their occupations, lifestyles, and even social activities [13], [14]. Therefore, there is an urgent demand for authenticating each other's identity, encrypting communication data, and protecting personal privacy while securely transferring charging information.

Currently, there are many solutions to EV identity authentication [12], charging information encryption [15], and personal privacy protection [16]. Nevertheless, these solutions are still imperfect because of the following two facts about the communication of charging information:

- In many cases, charging information are transmitted by public ISP networks, and there is no trusted third party (ISPs are untrusted in the view of grid companies) to authenticate identity, and to generate, distribute and manage encryption keys. This fact means that the solutions requiring a trusted third party [9] maybe inapplicable in practice.
- EVs, concentrator, and backend central system are often interconnected by wireless links. Therefore, massive charging information can be easily eavesdropped by attackers for later traffic analysis. Even worse, with advanced big data and signal processing technologies, attackers can not only infer a consumer's usage patterns, but also the approximate location of wireless terminals near that consumer, without decrypting the data payloads [17]. This fact substantially reduces the security of the solutions that mainly rely on encryption strategies to protect consumer privacy.

This paper proposes an innovative secure and anonymous communication scheme based on authentication and split transmission. This scheme improves the Diffie-Hellman protocol, which can achieve mutual authentication and resistance to man-in-the-middle attacks simultaneously without requiring a trusted third party. Furthermore, by splitting and forwarding charging information according to a pseudo-random table, our scheme ensures that the transmitted data have anonymous sources to resist traffic analysis.

To summarize, our main contributions are as follows.

- The proposed key distribution and authentication strategy, which innovatively incorporates the identity authentication into the key distribution protocol without the support of a third party, not only generates a session key that cannot be easily cracked, but also implements two-way secure access authentication for both parties. Moreover, because our strategy does not perform complicated encryption and decryption operations at EVs, it is applicable to real-world devices of EV that usually have very limited computation and storage capacity.
- We propose a novel split transmission strategy that can anonymously upload charging information from EVs to central system. Our strategy conceals the characteristics of each EV charging information by splitting the data into multiple fragments and forwarding them through several random communication links. For an eavesdropper listening to some of these links, it is nearly impossible to recover charging information and infer any sensitive information.

The rest of the paper is organized as follows. In Section 2, we highlight some related works in the literature. In Section 3, we introduce the system model that we attempt to secure. Section 4 presents details about our privacy-preserving schemes based on the improved Diffie-Hellman protocol and fragment transmission. The security level of our schemes in un-trustable environment is discussed in Section 5. Finally, we conclude the paper.

II. RELATED WORK

The communication links in smart grids are not absolutely trusted and are vulnerable to various attacks. In addition, the charging information transmitted in the smart grids often contains some private or sensitive information of both EV users and V2G service provider. Once intercepted, an attacker can use it to mine the user's occupation, lifestyle, and even social activities. Therefore, the secure and anonymous transmission of charging information in smart grids has attracted widespread attention from many researchers. At present, there are mainly four types of solutions for secure communication of consumption data: 1) access control; 2) anonymization; 3) data aggregation; and 4) mix in private energy.

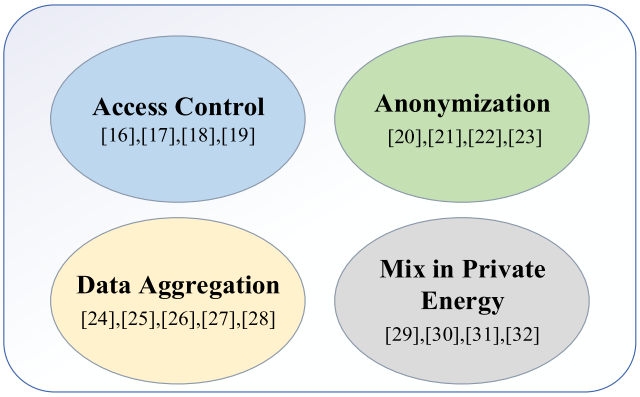


FIGURE 1. Classification of the state-of-the-art schemes.

The main idea of access control is to set a condition for the user in advance. The sensitive power consumption data can be accessed once the pre-set conditions are met. Otherwise the sensitive data cannot be accessed. Lewko *et al.* [18] proposed a CP-ABE mechanism based on the combination of bilinear group and dual-system encryption technology, which embeds user attributes in the key and theoretically proves its security. Bobba *et al.* [19] designed an online key distribution mechanism. With the online distribution of keys, it effectively reduces the risk of leaking sensitive data, and can resist selective ciphertext attacks. Ruj and Nayak [20] constructed a security architecture with both data aggregation and access control. The architecture is decentralized and combines the characteristics of homomorphic encryption and attribute-based encryption, so that participants with different

attributes in the smart grid can only access aggregated data with the same attributes. Hur [21] proposed a policy-hidden CP-ABE algorithm, which uses the CP-ABE algorithm to provide basic protection for user sensitive data. At the same time, the access control policy was hidden to avoid the possibility of user data leakage due to the leakage of the access control policy. While this type of method rejects the access of illegal users, it allows legitimate users to obtain other users' charging information, which is still risky in terms of privacy protection.

The main idea of anonymization is to destroy the correlation between electricity consumption and user identity. Efthymiou and Kalogridis [22] used a trusted third party to process the original user data, making it impossible for the power consumption data to correspond with the user's identity information. While anonymously protecting user data with privacy, there is a risk of transmitting malicious forged data. In response to this problem, Ren *et al.* [23] proposed a lightweight privacy protection scheme. It uses a third party to provide anonymization services for user data by using a hash function. Besides, the central system does not need to know the user's name when verifying the data. Diao *et al.* [24] proposed an anonymous certificate protocol based on Camenisch-Lysyanskaya signature. The protocol has controllable connectivity, which not only enables the central system to verify electricity consumption data without knowing the user's real identity, but also has the function of tracking bad data. Stegelmann *et al.* [25] proposed a GridPriv scheme, which is a k-anonymity-based privacy protection service architecture. When interacting with the central system, it allows k smart meters to share a pseudo-identity information, thereby protecting the user's identity information. Although such methods can effectively avoid the potential harm to the privacy of users caused by legitimate visitors, they require trusted third parties and large computation capacity, both of which are often unavailable in real-world smart grids.

The so-called data aggregation means that the central system only collects statistics of electricity consumption data. Lu *et al.* [26] designed a data aggregation protocol called EPPA, which uses homomorphic encryption technology to transmit encrypted data to the regional gateway. Due to the characteristics of homomorphic encryption, the regional gateway can directly perform aggregation operations on cipher text. On the one hand, it effectively prevents the central system from knowing the power consumption data of each user, and on the other hand, it prevents the possibility of the regional gateway from leaking the user's privacy. Kursawe *et al.* [27] used the Diffie-Helman key exchange protocol and bilinear mapping to enable the data center to obtain the final total electricity consumption without knowing the electricity consumption data of each specific user. Shi *et al.* [28] introduced the concept of homomorphic encryption technology and differential privacy, which not only ensured the privacy during data aggregation, but also achieved a measure of the degree of privacy protection. Erkin and Tsudik [29] proposed an efficient data aggregation mechanism that can complete data aggregation without a trusted third party. Li *et al.* [30] proposed a distributed incremental data aggregation method, which is also based on homomorphic encryption and uses a cleverly designed aggregation tree to aggregate electricity consumption data. With advanced big data and signal processing technologies, attackers can not only infer a consumer's usage patterns, but also the approximate location of wireless terminals near that consumer, without decrypting the data payloads. So, although the existing data aggregation-based privacy protection schemes can protect the privacy of power consumption data of users to a certain extent, the existing work still has a lot of room for improvement in resisting data analysis.

In addition, the literature [31]–[34] adopts the idea of mixing private energy, and uses the charge and discharge of rechargeable batteries to offset the electrical load so that the outside cannot detect the electrical characteristics of the electrical equipment. The algorithms proposed based on this idea include the Best-Effort (BE) algorithm, the Non-Intrusive Load Monitoring (NILL) algorithm, and a series of improved and extended algorithms based on these two algorithms. The idea of using private energy to offset the characteristics of electricity use is mainly based on the widespread application of the Non-Intrusive Load Monitoring (NILM) algorithm in smart grids. The NILM algorithm can analyze the power consumption of household users in detail, thereby obtaining a large amount of user behavior information. Although this method can ideally protect the charging information in an ideal state, it is impractical in many cases because most EVs nowadays are using replaceable battery instead of rechargeable battery.

In a word, existing works are either impractical or incapable for protecting charging information in many real-world scenarios. This situation motivates us to propose a new communication scheme that can securely and anonymously transmit charging information in practical smart grids, as discussed below.

III. THE FRAMEWORK OF V2G COMMUNICATION SYSTEM

In the V2G communication system, all user data is transmitted periodically through untrusted public networks. During the transmission process, data will be susceptive to malicious attacks such as identity forgery, man-in-the-middle attacks, and collusion attacks, which poses a huge threat to users' privacy and security. Aiming at the above problems, this paper starts from two perspectives of physical access and data transmission, and proposes a security and privacy protection scheme based on identity authentication and fragment transmission. This scheme uses the Diffie-Hellman protocol to dynamically generate session keys and complete secure access authentication. Adopting an anonymous data transmission strategy based on splitting and forwarding, the data collected by legal users is split and forwarded according to a pseudo-random table to ensure the indistinguishability of the data.

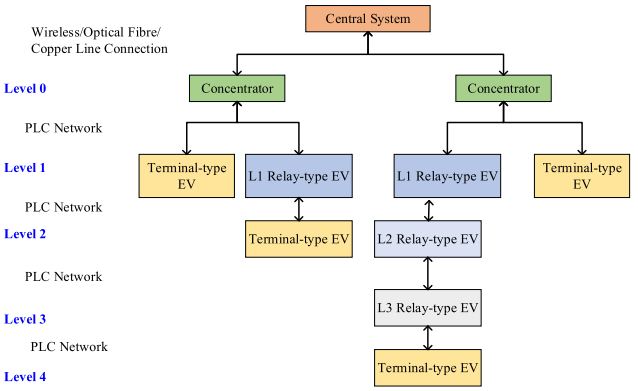


FIGURE 2. The framework of V2G communication system.

The V2G communication topology is built on the power-line communication (PLC) network. PLC has the advantage which can use the medium for power transmission to establish a communication network and transmit data. As shown in Figure 2, the framework of V2G communication system is consists of four parts, i.e., the terminal-type EV, the relay-type EV (L1 relay-type EV, L2 relay-type EV....), the concentrator, and the central system. Each EV is equipped with an onboard unit, which can support communication between the EV and the concentrator or other EVs. Both the terminal-type EV and the relay-type EV are all conventional EVs, just in different roles.

The terminal-type EV are the main members of V2G, which acts as a demand node. When the EV needs to be charged or discharged, it will need to interact with the grid. We denote electric vehicles that have the need to be connected to the grid as terminal-type EV. In addition, EV batteries can play an important role in the large-scale power access of renewable energy. This not only improves the stability of the smart grid, but also reduces the investment of the smart grid in reserve capacity and equipment transformation.

The relay-type EV are regular EV, which acts as a gateway for other EVs. Generally, each EV is associated with a concentrator, which controls the permission of each EV sending its data. However, EVs cannot be directly connected to the concentrator in some special cases (e.g., the distance is too far, or the signal is too weak). At the cases, it can use other EVs as relay nodes to obtain links with the concentrator. The EV as a relay node is named as a relay-type EV which is hierarchical. Among them, the EV directly connected to the terminal-type EV is called the L3 relay-type EV. The EV directly connected to the concentrator is called the L1 relay-type EV. Besides, the relay-type EV located between the L1 relay-type EV and the L3 relay-type EV is called the L2 relay-type EV.

The concentrator is an intermediate connection device between an EV and a central system. It collects charging information from associated EVs and regularly transmits them to the central system by wired communication. The concentrator able to send instructions, such as requesting EV charging information or turning off power. The concentrator is configured by the control center and automatically run after configuration. With the help of the concentrator, the V2G communication system can be divided logically into smaller components, which can realize the automatic domination of various regions. To some extent, the concentrator alleviates the network congestion caused by the central system collecting data in real time.

The central system collects the data sent by concentrator and then processes and analyzes them, which are useful for the electricity supplier in making decisions such as scheduling and pricing. Due to legal regulations, these data must be deleted within the specified interval.

IV. SECURE AND ANONYMOUS COMMYNICATION SCHEME

A. MUTUAL AUTHENTICATED KEY AGREEMENT SCHEME (MAKA)

To securely transmit charging information, EV and concentrator (and similarly concentrator and central system) must authenticate each other's identity and agree on a secret key. Here we propose a new strategy that can simultaneously perform identity authentication and key distribution based on Diffie-Hellman protocol without a trusted third party, as illustrated by Figure 3.

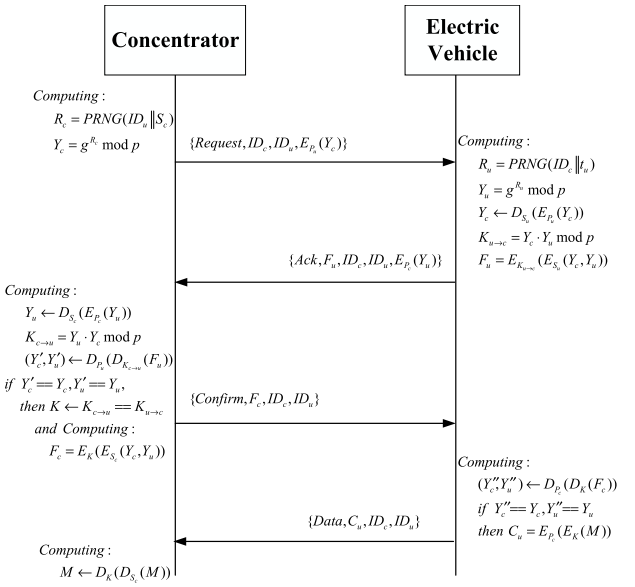


FIGURE 3. Identity authentication and key agreement strategy between electric vehicle and concentrator (This strategy can also be used for concentrator and central system).

Each EV will register a non-overlap certificated number ID_u, and the concentrator has a backup of each user's certificated number. The concentrator and EVs have their own public and private keys, which are P_c, S_c, P_u, and S_u. The public key is public, and the private key is only held by themselves. To facilitate the description of the strategy, we list the commonly used symbols in Table 1. The details of our strategy are presented below.

TABLE 1. Commonly used symbols.

Variable	Definition
ID_c	ID number of the Concentrator
ID_u	ID number of the Electric vehicle
S_c	The Private Key of Concentrator
P_c	The Public Key of Concentrator
S_u	The Private Key of Electric vehicle
P_u	The Public Key of Electric vehicle
Y_c	Key material generated by the Concentrator
Y_u	Key material generated by the Electric vehicle
R_c	Random number generated by the Concentrator
R_u	Random number generated by the Electric vehicle
F_c	Concentrator confirmation factor
F_u	Electric vehicle confirmation factor
t_u	Timestamp
$K_{c\to u}$	The concentrator-side secret key
$K_{u\to c}$	The electric vehicle-side secret key
K	Negotiated keys
g, p	Parameters of the Diffie-Hellman key exchange protocol
PRNG (.)	A Pseudo Random Number Generator that generates random number
E (.)	An encryption algorithm that converts plaintext into ciphertext
D (.)	A decryption algorithm that converts ciphertext into plaintext

1) REQUEST COMMAND FROM CONCENTRATOR

When a concentrator intends fetch charging information from an EV, it first sends a request command to the EV. The command $Request, ID_c, ID_u, E_{P_u}(Y_c)\}$ contains the request information of the concentrator, the respective certificate numbers of the concentrator and the EV, and a key material encrypted by the EV's public key. This key material is unique to each EV, and we will introduce how it is obtained later.

With the help of a Pseudo Random Number Generator (PRNG), the concentrator first generates a unique random number R_c by using its own private key S_c and the target EV's ID ID_u as input:

$$R_c = PRNG(S_c \parallel ID_u) \tag{1}$$

Then, based on the random number R_c, the concentrator gets the key material Y_c using the well-known Diffie-Hellman key exchange protocol [35]:

$$Y_c = g^{R_c} mod p \tag{2}$$

where g and p are the parameters of the Diffie-Hellman key exchange protocol, p is a prime number, and g is the primitive root of p.

2) ACK MESSAGE FROM ELECTRIC VEHICLE

When the EV receives the request message $\{Request, ID_c, ID_u, E_{P_u}(Y_c)\}$ from the concentrator, it sends a corresponding ACK message $Ack, F_u, ID_c, ID_u, E_{P_c}(Y_u)$. The ACK message contains the EV's response information, an acknowledgement factor F_u that is double-encrypted by the EV's private key S_u and the EV-side secret key $K_{u\to c}$, the control certificated number of the concentrator and the EV, and the key material Y_u encrypted by the concentrator's public key P_c.

The EV first generates a timestamp t_u, and then generates a random number R_u by using a PRNG based on the timestamp and the ID number of the concentrator ID_c.

$$R_u = PRNG(t_u \parallel ID_c) \tag{3}$$

Note that the EV does not generate the next timestamp until it has new data for encryption. Therefore, the timestamps of the EV continuously change with time. In other words, the timestamps are different for different data transmissions.

Similar to (1), the EV generates its key material Y_u using the Diffie-Hellman key exchange protocol according to the calculated random number R_u.

$$Y_u = g^{R_u} mod p \tag{4}$$

In addition, the EV decrypts the encrypted information in the request command, thereby obtaining the concentrator's key material Y_c. The EV-side secret key $K_{u\to c}$ is obtained by connecting the Y_c and its $Y_u$as input through the Diffie-Hellman protocol. Finally, encapsulate Y_c and Y_u together, then encrypt it twice with $K_{u\to c}$ and the EV's private keys S_u respectively. We call this double encryption result as the EV-side confirmation factor, use F_u to represent it.

$$F_u = E_{K_{u\to c}}(E_{S_u}(Y_c, Y_u)) \tag{5}$$

3) AUTHENTICATING ELECTRIC VEHICLE'S IDENTITY

After receiving the ACK message, the concentrator first uses its private key to decrypt the key material and obtains Y_u. Then the concentrator combines Y_u with its Y_c, uses the Diffie-Hellman protocol to get the concentrator-side secret key $K_{c\to u}$. To authenticate the identity of the EV, the concentrator uses the $K_{c\to u}$ and the public key of EV to decrypt the EV-side confirmation factor (to denote the results as Y_c' and Y_u' respectively) and compare the decrypt results with Y_c, Y_u. If the two sets of values are equal, the identity of the EV is legal. Then the concentrator calculates the concentrator-side confirmation factor F_c.

$$F_c = E_{K_{c\to u}}(E_{S_c}(Y_c, Y_u)) \tag{6}$$

Now the concentrator has authenticated the identity of the electric vehicle. Henceforth, it sends a confirmation message $Confirm, F_c, ID_c, ID_u$ to the EV.

4) AUTHENTICATING CONCENTRATOR'S IDENTITY

The EV also needs to authenticate the identity of the concentrator. The EV decrypts the concentrator's confirmation factor to obtain Y_c'' and Y_u'' by using the $K_{u\to c}$ and the public key of concentrator. Afterwards, it compares the obtained set of values Y_c'' and Y_u'' with its original values Y_c, Y_u. If the two sets of values are equal, the identity of the concentrator is considered correct.

So far, the EV and the concentrator have authenticated each other's identity.

5) ESTABLISHING SESSION KEY BETWEEN ELECTRIC VEHICLE AND CONCENTRATOR

While EV and concentrator implement mutual authentication of identities, they also obtain their own secret keys, namely $K_{u\to c}$ and $K_{c\to u}$. It can be seen that $K_{u\to c}$ and $K_{c\to u}$ are equal, and they are uniformly referred to as K here. K is negotiated by EVs and concentrators, both of which do not know what the key to be generated looks like at all before the key is generated. Therefore, this scheme uses K as the session key between the EV and the concentrator, then uses it to encrypt the communication content between them to ensure its security.

B. ANONYMOUS DATA TRANSMISSION BASED ON SPLITTING AND FORWARDING

Aiming at the privacy protection of massive power consumption information easily eavesdropped by attackers for later traffic analysis, we design an anonymous data transmission scheme based on splitting and forwarding. The scheme consists of three stages. First, it initializes the system parameters. Secondly, the concentrator constructs a pseudo-random schedule, then encrypts and distributes them to each EV. At last, EV splits data and completes the data forwarding according to the forwarding pseudo-random schedule. The details of our strategy are presented below.

1) INITIALIZATION

Each concentrator will build a cluster for the nearby EVs before transmitting electricity information to them. The specific formation process of the cluster is shown in Figure 5. The concentrator sends the message HELLO to all EVs in its coverage area, and an EV selectively sends a JOIN message to respond to the concentrator's HELLO message. In general, EVs should join multiple clusters whenever possible. As can be seen from Figure 5, EV_1 can join two clusters built by concentrator C_1 and C_2 simultaneously. Similarly, EV_3 can join two clusters constructed by concentrator C_2 and C_3. By the same token, it can be known that EV_2 can simultaneously be a member of three clusters built from concentrator C_1, C_2 and C_3. The cluster size constructed by each concentrator is denoted as n, where n refers to the number of EVs in the cluster. A cluster i with n wireless terminals (including EV and concentrator) is written as C_i=(v_{i1}, v_{i2}, .., v_{in}).

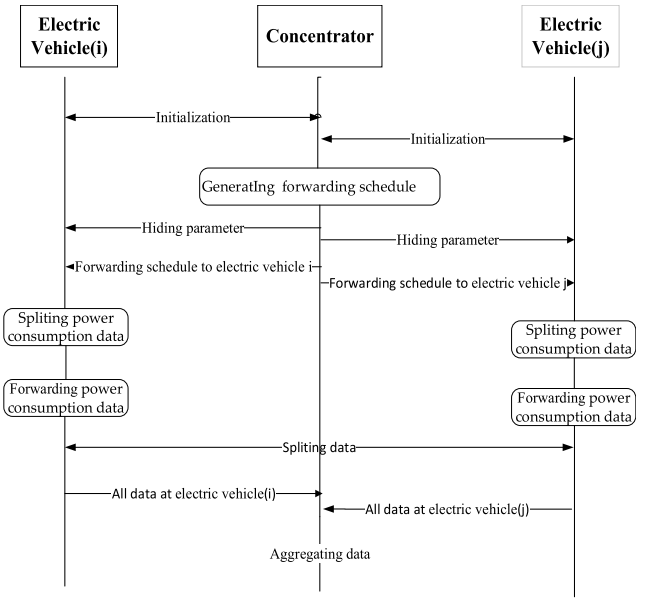


FIGURE 4. Anonymous transmission scheme.

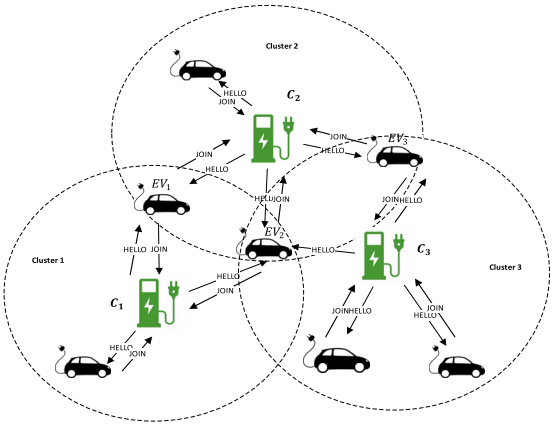


FIGURE 5. Cluster formation for anonymous data transmission.

When the cluster is built, the concentrator determines adaptively the number to be split for each transmitting data based on the current traffic load and security level of the communication link between it and EV. The splitting number of a data is denoted as s. For a concentrator, the smaller the value of s, the smaller the computational overhead of data reassembly. For wireless terminals, the larger s, the better the privacy protection effect on the data.

2) GENERATING FORWARDING SCHEDULE

In the proposed anonymous data transmission scheme, each EV has an exclusive forwarding schedule. The forwarding schedule is composed of random numbers. The probability of all numbers in the schedule appearing at any position is equal. The electric vehicle forwards each split data based on the forwarding schedule, which not only ensures that the trace of data forwarding is irregular, but also ensures that the number of split data received by each EV in the cluster is equal, i.e., load balancing.

The generation of the forwarding schedule is divided into three stages, i.e., build a random seed array, generates an irregular matrix set, and assigns forwarding schedule for each electric vehicle within the cluster. The generation process of the forwarding schedule is shown in Figure 6.

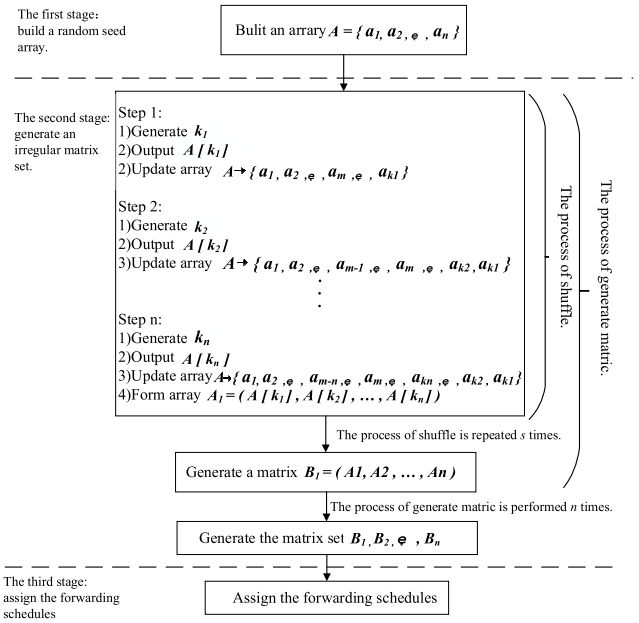


FIGURE 6. The process of generating forwarding schedule.

In the first stage, to ensure the randomness of the elements in the forwarding schedule, the concentrator builds a random seed array A with m ($m \geq n$) elements, each of which is given an integer between 1 and m in turn, $A = \{a_1, a_2, \ldots a_m\}$.

In the second stage, the concentrator generates a set of matrices that are different from each other, in order to ensure that each member of the cluster has an exclusive forwarding schedule and that the number of split data received by each EV in the cluster is equal. The specific generation process is as follows. First, we generate a random number k_1 ranging from [0, $m-1$] with the help of a random number generator. The (k_1+1)-th element in array A ($A[k_1]$) is used as the first random number, and then we swap it with the last element in array A. In like manner, we can get another random number k_2 ranging from [0, $m-2$]. The (k_2+1)-th element in array A ($A[k_2]$) is used as the second random number, and then we swap it with the last but one element in array A. Then, the above steps are repeated until n numbers are output. The generated n random numbers are formed into the new array $A1 = (A[k_1], A[k_2], \ldots, A[k_n]), i \in [1, n], k_i \in [1, m]$. We call the above process as shuffling, then the process is repeated s times to generate a matrix B_1 of s^*n, B_1=($A1, A2, .., An$). After that, this process of generating matric is performed n times to obtain the matrix set $B_1, B_2, .., B_n$.

In the third stage, we take the j-th matrix ($j \in [1,n]$) from this set and use them as the forwarding schedule for the j-th EV within the cluster i.

The concentrator uses the session key negotiated during identity authentication to encrypts each forwarding schedule and hidden parameter obtained by initialization, then sends them to the dedicated EVs.

3) SPLITTING AND FORWARDING DATA

Here, we can denote the data collected by the EVv_{ix} as $D_{ix}(x \in [1, n])$. The system usually sets some collection time in advance. So, the EV will split the D_{ix} according to the received initialization parameters when the timestamp reaches the collection threshold. D_{ix} is split into $d_{i1}, d_{i2} \ldots d_{is}$ and the relationship between them can be expressed by the following equation.

$$D_{ix} = (\sum_{j=1}^{s-1} d_{ij}) \times d_{is}, i, d_{ij} \in Z, \quad j \in [1, s] \qquad (7)$$

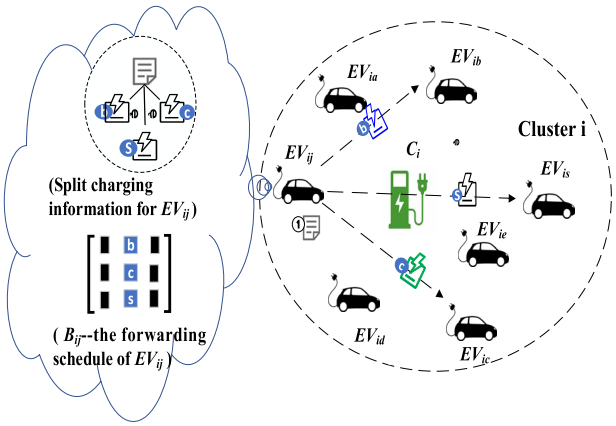


FIGURE 7. The process of forwarding sliced data.

After splitting the data, the next step is to forward the sliced data irregularly that the process of forwarding sliced data is shown in Figure 7. The EV stores its own unique random forwarding schedule. When the scheduled time to upload data is reached, each EV extracts the scheduled time stamp t and then takes the corresponding number in column *tmodn* of $B_{ij}, i \in Z, j \in [1, n]$ as the forwarding node to forward the sliced data. Here we take the electric vehicle $EV_{ij}(v_{ij})$as an example, if the elements in column *tmodn* of B_{ij} (the forwarding schedule of EV_{jj}) are $b, c, \ldots$ and s. The EV v_{ij} stores d_{i1} by himself and sends the other slices of data ($d_{ib}, d_{ic} \ldots d_{is}$) to the electric vehicles $v_{ib}, v_{ic} \ldots v_{is}$ in turn. Other EVs do the same thing as EV v_{ij}. In this way, the concentrator gets the aggregated data of all EVs at time t, and it cannot get the power consumption of each EV. In addition, each EV cannot know the power of other EVs.

The data is transferred between the EV and the concentrator using the PLC network. The concentrators are connected to the central system through wireless or wired connections.

V. PERFORMANCE ANALYSIS

This section will conduct a security analysis of our solution, and explain how our solution achieves user privacy-preserving and lightweight goals.

A. SECURITY OF IDENTITY AUTHENTICATION AND KEY AGREEMENT

Identity authentication is the basis for the implementation of all other security measures in the communication network. We innovatively incorporate the identity authentication into the Diffie-Hellman protocol. By simulating the principle of three-way handshake, this solution realizes the access authentication of both communication parties while negotiating the key. In addition to achieving identity authentication and data confidentiality, the solution can also resist man-in-the-middle attacks and replay attacks.

1) IDENTITY AUTHENTICATION

When the EV accesses to the concentrator, the identity authentication is implemented as follows:

$$\begin{aligned} D_{P_u}(D_{K_{c\to u}}(F_u) &\to \left(Y_c', Y_u'\right) \\ &= (g^{R_c} modp, g^{R_u} modp) \\ &= (Y_c, Y_u) \end{aligned}$$

The EV will verify the identity when it receives the correctness's confirm message. The correctness of the identity will be verified as follow:

$$\begin{aligned} D_{P_u}(D_{K_{u\to c}}(F_c) &\to \left(Y_c'', Y_u''\right) \\ &= (g^{R_c} modp, g^{R_u} modp) \\ &= (Y_c, Y_u) \end{aligned}$$

Thus, this solution achieves mutual authentication between concentrator and EV.

2) DATA CONFIDENTIALITY

In our solution, session key is generated by Y_c and Y_u, which respectively generated by R_c (the random number of concentrator) and R_u (the random number of EV). It is noteworthy that, R_c is generated based on EV's ID number and the private key of concentrator (S_c), which is impossible to be obtained in public network. R_u is a random number generated by EV's timestamp t_u, and is also statistically impossible to be recovered. In addition, given the difficulty of discrete logarithmic calculation in Galois field, it is extremely difficult to infer R_c and R_u in reverse order even if Y_c and Y_u is obtained.

Moreover, the session key is one-off in our scenario, i.e., it is different for each session. This is because a part of the session key R_u is generated based on the timestamp t_u that varies quickly over time. Therefore, even if a piece of encrypted user data is cracked by chance, the subsequent data can still be securely transmitted for the session key have already changed.

In summary, the encrypted data in V2G are difficult for attacker to crack, and the session key keeps changing over time. Therefore, the confidentiality of data transmission is guaranteed.

3) RESISTANCE TO REPLAY ATTACKS AND MAN-IN-THE-MIDDLE ATTACKS

Furthermore, our scheme can resist some other attacks, e.g., replay attack and man-in-the-middle attack. In our scheme, we first use the communication party's public key (P) to asymmetrically encrypt the key material (Y) and then transmit it, which avoids malicious attackers from eavesdropping and tampering with the key material. Since R_u is generated based on timestamps t_u that has dynamic variability, so the scheme can resist replay attack. During the key agreement process, the scheme uses the confirmation factors F_u and F_c to confirm the authenticity of both parties' identities, which effectively prevents man-in-the-middle attack.

B. ANONYMITY OF TRANSMITTING CHARGING INFORMATION

With the development of big data and machine learning technologies, some attackers are able to perform feature extraction and data classification on the encrypted data without cracking them. The classified encrypted data may leak out some sensitive information of EV, such as the identity of the EV, the electricity consumption pattern of EV.

Our secure transmission scheme overcomes the problem of only using encryption methods to protect privacy. It randomly divides the data into s data fragments through the data multiplication algebra operation $D_{ix} = (\sum_{j=1}^{s-1} d_{ij}) \times d_{is}$ and transmits the encrypted data fragments randomly according to the pseudo-random table. This transmission process makes the data indistinguishable, that is, the characteristics of the original data are destroyed. Even if the attacker intercepts and restores the data transmitted by the individual, it is impossible to infer the true data and data range of the EV based on this. Therefore, the security transmission scheme proposed in this article can effectively prevent data features from being extracted, thereby effectively preventing the leakage of individual privacy.

C. COMPUTATION COMPLEXITY

In our scheme, the session key is dynamically generated when needed, thus EV does not need any key storage. In addition, the computation overhead of wireless terminals mainly comes from data splitting operations and encryption operations on sliced data. Data slicing uses data addition and multiplication algebra operations, so its computation complexity is merely $o(1)$. The encryption operation of the sliced data uses a symmetric encryption algorithm, which can be easily performed with little computational overhead. Therefore, our solution is lightweight for EVs with limited storage and computing capabilities.

VI. CONCLUSIONS

Aiming at the problem about safe transmission of charging information in V2G, this paper proposes a lightweight privacy protection scheme based on the improved Diffie-Hellman protocol and fragment transmission. This scheme uses the Diffie-Hellman protocol to dynamically generate session

keys and complete secure access authentication. Adopting an anonymous transmission strategy based on data splitting and forwarding, the data collected by legal users is split and forwarded according to a pseudo-random table to ensure the indistinguishability of the data. The security performance analysis shows that the proposed scheme has the following advantages compared with the commonly used privacy protection scheme: resistant to data analysis, lightweight, no need for trusted third-party support, anti-man-in-the-middle attack, and the advantage of helping the central system to connect more users.

REFERENCES

[1] Y. Liu, "Big data technology and its analysis of application in urban intelligent transportation system," in *Proc. Int. Conf. Intell. Transp., Big Data Smart City (ICITBS)*, Xiamen, China, Jan. 2018, pp. 17–19.

[2] Z. Ning, K. Zhang, X. Wang, S. Mohammad Obaidat, L. Guo, X. Hu, B. Hu, Y. Guo, B. Sadoun, and Y. K. Ricky Kwok, "Joint computing and caching in 5G-envisioned Internet of vehicles: A deep reinforcement learning based traffic control system," *IEEE Trans. Intell. Transp. Syst.*, early access, Feb. 5, 2020, doi: 10.1109/TITS.2020.2970276.

[3] H. Ben Sassi, F. Errahimi, N. Essbai, and C. Alaoui, "V2G and wireless V2G concepts: State of the art and current challenges," in *Proc. Int. Conf. Wireless Technol., Embedded Intell. Syst. (WITS)*, Fez, Morocco, Apr. 2019, pp. 1–5.

[4] J. Y. Yong, V. K. Ramachandaramurthy, K. M. Tan, and N. Mithulananthan, "A review on the state-of-the-art technologies of electric vehicle, its impacts and prospects," *Renew. Sustain. Energy Rev.*, vol. 49, pp. 365–385, Sep. 2015.

[5] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Trans. Veh. Technol.*, early access, Feb. 28, 2020, doi: 10.1109/TVT.2020.2976960.

[6] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vols. 91–92, pp. 17–28, Jun. 2016.

[7] H. Liu, Z. Hu, Y. Song, and J. Lin, "Decentralized Vehicle-to-Grid control for primary frequency regulation considering charging demands," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3480–3489, Aug. 2013.

[8] Z. Ning, K. Zhang, X. Wang, L. Guo, X. Hu, J. Huang, B. Hu, and R. Y. K. Kwok, "Intelligent edge computing in Internet of vehicles: A joint computation offloading and caching solution," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 5, 2020, doi: 10.1109/TITS.2020.2997832.

[9] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart Vehicle-to-Grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[10] T. Hartmann, "Generating realistic smart grid communication topologies based on real-data," in *Proc. Smart Grid Comm*, Venice, Italy, 2014, pp. 428–433.

[11] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[12] N. Saxena and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1438–1452, Jul. 2016.

[13] M. H. Eiza, Q. Shi, A. K. Marnerides, T. Owens, and Q. Ni, "Efficient, secure, and privacy-preserving PMIPv6 protocol for V2G networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 19–33, Jan. 2019.

[14] M. He, K. Zhang, and X. S. Shen, "PMQC: A privacy-preserving multi-quality charging scheme in V2G network," in *Proc. IEEE Global Commun. Conf.*, Austin, TX, USA, Dec. 2014, pp. 675–680.

[15] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social Internet of Things," *IEEE Access*, vol. 7, pp. 76812–76832, 2019.

[16] P. Gope and B. Sikdar, "Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1554–1566, Jun. 2019.

[17] C. Cheng, J. Lee, T. Jiang, and T. Takagi, "Security analysis and improvements on two homomorphic authentication schemes for network coding," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 993–1002, May 2016.

[18] A. Lewko, T. Okamoto, and A. Sahai, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Germany, 2010, pp. 62–91.

[19] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf, "PBES: A policy based encryption system with application to data sharing in the power grid," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur.*, 2009, pp. 262–275.

[20] S. Ruj and A. Nayak, "A decentralized security framework for data aggregation and access control in smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[21] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[22] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Feb. 2010, pp. 238–243.

[23] W. Ren, J. Song, Y. Yang, and Y. Ren, "Lightweight privacy-aware yet accountable secure scheme for SM-SGCC communications in smart grid," *Tsinghua Sci. Technol.*, vol. 16, no. 6, pp. 640–647, Dec. 2011.

[24] F. Diao, F. Zhang, and X. Cheng, "A privacy-preserving smart metering scheme using linkable anonymous credential," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 461–467, Jan. 2015.

[25] M. Stegelmann and D. Kesdogan, "Gridpriv: A smart metering architecture offering k-anonymity," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, 2012, pp. 419–426.

[26] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[27] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, Berlin, Germany, 2011, pp. 175–191.

[28] E. Shi, "Privacy-preserving aggregation of time-series data," in *Proc. Annu. Netw. Distrib. Syst. Secur. Symp.*, 2011, pp. 1–17.

[29] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, Berlin, Germany, 2012, pp. 561–577.

[30] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 327–332.

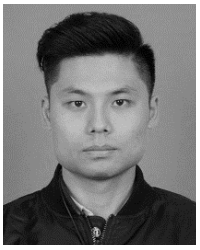
[31] I. Natgunanathan, M. B. Hossain, Y. Xiang, L. Gao, D. Peng, and J. Li, "Progressive average-based smart meter privacy enhancement using rechargeable batteries," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9816–9828, Dec. 2019.

[32] J. Yang, G. Huang, and C. Wei, "Privacy-aware electricity scheduling for home energy management system," *Peer Peer Netw. Appl.*, vol. 11, no. 2, pp. 309–317, Mar. 2018.

[33] G. Giaconi, D. Gunduz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 129–142, Jan. 2018.

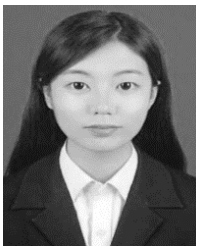
[34] E. Liu and P. Cheng, "Achieving privacy protection using distributed load scheduling: A randomized approach," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2460–2473, Sep. 2017.

[35] P. Deshpande, S. Santhanalakshmi, P. Lakshmi, and A. Vishwa, "Experimental study of diffie-hellman key exchange algorithm on embedded devices," in *Proc. Int. Conf. Energy, Commun., Data Analytics Soft Comput. (ICECDS)*, Chennai, India, Aug. 2017, pp. 2042–2047.



JINGTANG LUO (Member, IEEE) received the B.Eng. and Ph.D. degrees in communication and information system from the University of Electronic Science and Technology of China, Chengdu, China, in 2011 and 2016, respectively. He is currently a Researcher with the State Grid Sichuan Economic Research Institute, Chengdu. His current research interests include communication networks, information security, and artificial intelligence in power systems. He serves as a Reviewer for international academic journals, including the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and the *Journal of Computer Science and Technology*.

SHIYING YAO received the M.E. degree in instrument science and technology from Chongqing University, Chongqing, China, in 2003. She is currently a Researcher with the State Grid Sichuan Economic Research Institute, Chengdu, China. She had published nine articles. She holds two Chinese patents in the field of communication network. Her research interest includes communication and automation technologies for power systems.



JIAMIN ZHANG received the M.S. degree from Shenyang Ligong University, Shenyang, China, in 2018. She is currently pursuing the Ph.D. degree in communication and information engineering with the University of Science and Technology Beijing, Beijing. Her research interests include security of networks and information, anonymous communication, and privacy protection.

WEITING XU received the B.Eng. and Ph.D. degrees in power system automation from Sichuan University, Chengdu, China, in 2008 and 2013, respectively. He is currently a Researcher with the State Grid Sichuan Economic Research Institute, Chengdu. His research interests include power gird planning and power system stability and security.

YUN HE received the M.S. degree from the China University of Mining and Technology at Beijing, Beijing, China, in 2016. She is currently pursuing the Ph.D. degree in communication and information systems with the University of Science and Technology Beijing, Beijing. Her research interests include security of networks and information, anonymous communication, and privacy protection.

MIN ZHANG (Member, IEEE) is currently an Associate Professor with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China. She has fulfilled more than ten research projects, including the National Natural Science Foundation of China and the National Hi-Tech Research and Development Program (863 Program). She has authored more than 60 articles. She holds 30 patents. Her research interests include content distribution networking and network security.