Privacy Preservation for V2G Networks in Smart Grid: A Survey

Wenlin Han[a], Yang Xiao[a,*]

[a]*Department of Computer Science*
The University of Alabama
Tuscaloosa, AL, 35487-0290 USA
emails: whan2@crimson.ua.edu, yangxiao@ieee.org

Abstract

Vehicle to grid (V2G) network is a crucial part of smart grid. An electric vehicle (EV) in a V2G network uses electricity instead of gasoline, and this benefits the environment and helps mitigate the energy crisis. By using its battery capacity, the vehicle can serve temporarily as a distributed energy storage system to mitigate peak load of the power grid. However, the two-way communication and power flows not only facilitate the functionality of V2G network, but they also facilitate attackers as well. Privacy is now a big obstacle in the way of the development of V2G networks. The privacy preservation problem in V2G networks could be more severe than in other parts of Smart Grid due to its e-mobility. In this paper, we will analyze and summarize privacy preservation approaches which achieve various privacy preservation goals. We will survey research works, based on existing privacy preservation techniques, which address various privacy preservation problems in V2G networks, including anonymous authentication, location privacy, identification privacy, concealed data aggregation, privacy-preserving billing and payment, and privacy-preserving data publication. These techniques include homomorphic encryption, blind signature, group signature, ring signature, third party anonymity, and anonymity networks. We will summarize solved problems and issues of these techniques, and introduce possible solutions for unsolved problems.

Keywords: Privacy preservation, Smart Grid, V2G networks, Security

1. Introductions

The traditional power system distributes electricity from power generation plants to the end consumers in one direction, which is inefficient and unreliable since it cannot satisfy the increasing future demand and the system is lacking efficient monitoring and quick response, easily resulting in power outages. As reported in the paper [1], the cost is approximate 100 billion dollars each year for power outages in US traditional power systems. Smart Grid provides two-way electricity flow and data communication. The two-way electricity flow incorporates distributed renewable energy better, such as solar and wind energy, which benefits both environmental protection and the mitigation of the energy crisis [2]. The two-way data communication provides intensive system monitoring and quick system recovery.

Vehicle to grid (V2G) network is one of the significant parts of Smart Grid, together with Home Area Network (HAN) [4], Industry Area Network (IAN), Neighborhood Area Network (NAN) [5, 6, 7, 8], and Building Area Network (BAN) [2]. As shown in Fig. 1, a V2G network describes a system where electric vehicles (EVs) communicate with service providers via aggregators (LAGs)

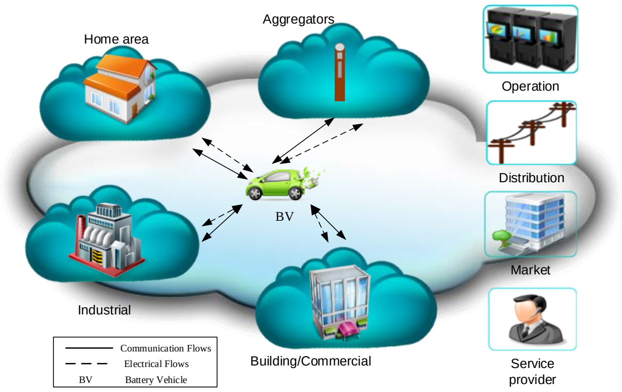

Figure 1: The role of V2G networks in Smart Grid.

[*] Corresponding author, Phone: 1-205-348-4038; Fax: 1-205-348-6959; email: yangxiao@ieee.org.

Preprint submitted to Journal of LaTeX Templates *April 24, 2016*

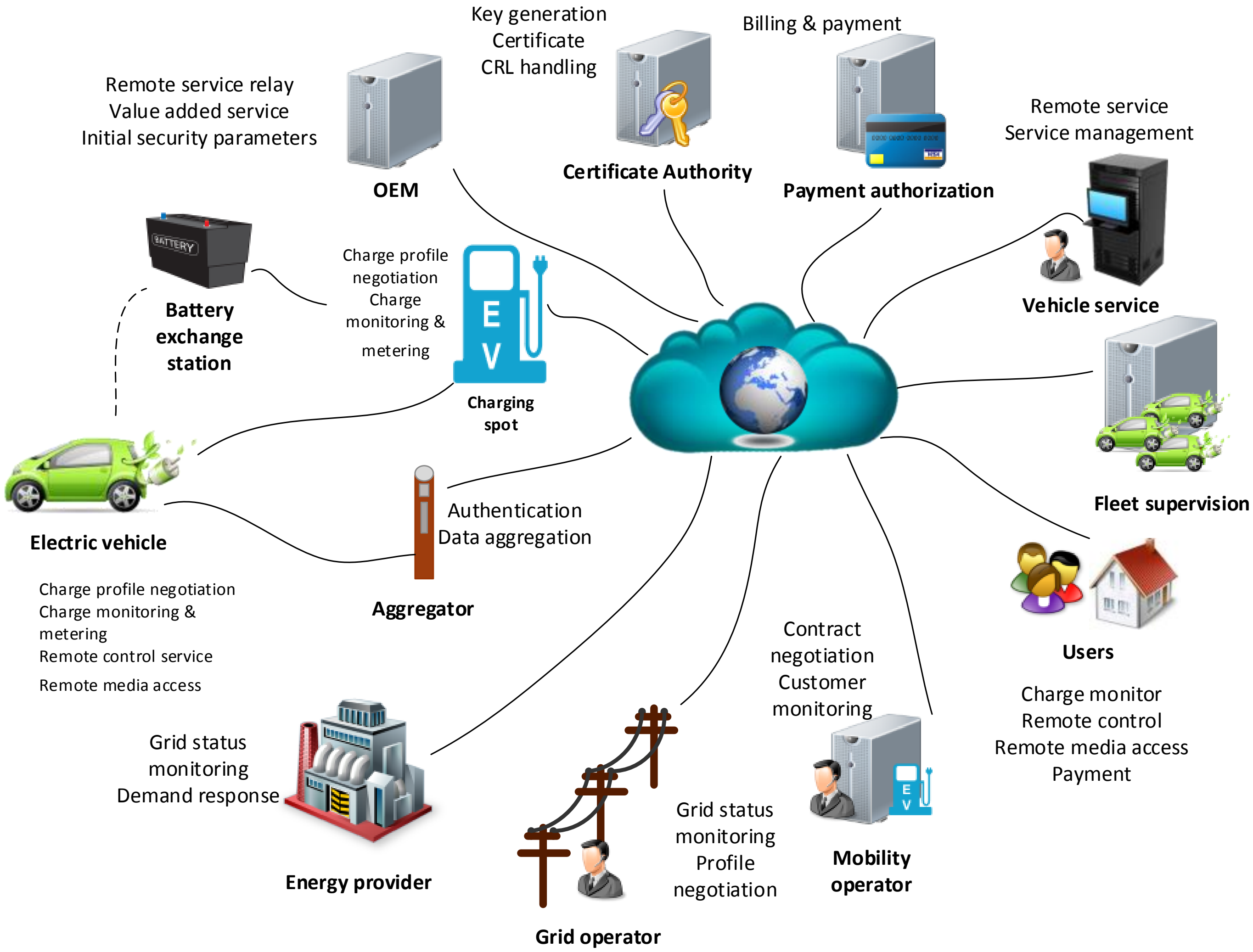

Figure 2: V2G networks framework and components [3].

or other networks, such as HANs. The functions of an LAG include aggregation of information and communication among entities. Fig. 2 shows the infrastructure of V2G networks, including power services for EVs and value-added services. The variety of entities in the infrastructure including Certificate Authority (CA), vehicle service, charging spot, etc. Charging spots act as energy access points for an EV to connect to the power grid or other EVs for charging or discharging. One reason why an EV sometimes discharges electricity back to the grid is due to the different prices at different times of a day [4], e.g., the EV can charge itself during night time with a lower price and discharge it back to the grid with a high price during the day. Energy providers and grid operators connect to the power grid for energy generation, transmission, and distribution [9]. Battery exchange stations provide fully charged batteries to battery-installed vehicles. Payment authorization and mobility operators are in charge of billing related services. Vehicle service and fleet supervision manage traffic related services of EVs. CA stores keys and certificates of all the entities. When services are outsourced, the Original Equipment Manufacturer (OEM) is responsible for service relay and value added services. An LAG aggregates information and energy collected from EVs and sends to corresponding entities.

The development of V2G networks will affect our personal lives. Firstly, from the angle of environmental protection, V2G networks will greatly accelerate the process. Renewable energy, such as wind power and solar power, has been introduced, developed, and exist for a long time, but the effect is not as expected. We still rely on the traditional power source, such as gas and carbon, which are not environment-friendly and non-renewable. The reason is that it is costly to build a large wind power generation station, and not every house owner is interested in installing a small wind power generator. V2G networks employ EVs, which can be powered by solar plates and can sell excessive electricity back to the grid to make money, or to power home appliances. Secondly, it is a good solution to the energy crisis. Every day, vehicles around the world consume a lot of gas and oil, which are non-renewable energy. The energy crisis will accelerate with the increase of these vehicles. The more vehicles join V2G networks using renewable energy, the quicker the energy crisis could be mitigated. Thirdly, the two-way electricity flow allows vehicle owners to save their budgets and even make money by selling electricity. Last, but not the least, EVs act as distributed battery storage systems, using their excess battery capacities to provide energy to the power grid to leverage demands during peak load periods.

There is not a universal definition for privacy since it means different things to different people. In our understanding, privacy can be seen as the right to be left alone. Private information should be kept confidential, but privacy preservation is not equal to confidentiality. Respect for persons and beneficence are two principles of the Belmont Report [10] and support both privacy and confidentiality. But confidentiality is to limit access or place restrictions on certain types of data, and privacy often relates to anonymity, which means remaining unidentified or unnoticed in a public area. For example, in a lot of applications, some data are provided to another party without confidentiality while meantime some sensitive personal information inside the provided data should be anonymized to provide privacy [11], [12], [13].

Privacy concern is now one big obstacle to the success of V2G networks, as well as Smart Grid. Protesters never give up their protests to stop Smart Grid. Protesters disrupted the Smart Grid conference held in Los Angeles [14]. In March 2013, Massachusetts residents spoke out about Smart Grid pilot of National Grid in Worcester, referencing the program's possible privacy concerns, health risks, and costly implementation [15]. Many other similar protests have taken place all over the world, including Canada, Germany, and other European Union countries [16]. There is even an organization, named Stop Smart Meters [17].

The two-way communication and electricity flows significantly improve the efficiency, reliability, and flexibility of Smart Grid and V2G networks, but they also raise great security issues and challenges of privacy preservation. Normally, metering data are read on a monthly basis in traditional power systems, but more granular and detailed energy usage data are read using smart meters approximately every 15 minutes or less in Smart Grid [18]. These data might potentially expose a large amount of personal information of customers, including patterns of energy usage, types of household appliance, the number of people in a household, along with their schedules or activities. Utility companies and appliance manufacturers can benefit from these personal data, which customers may not want to reveal. Attackers can eavesdrop the network and compromise the devices for a malicious purpose, causing economic loss or other negative results. In V2G networks, when a vehicle connects to a charging spot, data related to this vehicle and its owner are collected, as is another information like location and payment. It means that when you travel, an adversary may pinpoint where you are. On the one hand, utility companies need some of the information to monitor the grid and to respond to emergencies and to recover the grid. On the other hand, customers have the right to keep their data private. Furthermore, most of the customers do not trust utility companies to collect these data.

Privacy preservation problems in V2G networks are more challenging than in other networks in Smart Grid, such as HAN, which is location-fixed. It is much more difficult for an adversary to compromise an appliance in your house than to compromise a charging spot or an LAG deployed along the road. Moreover, due to e-mobility, a vehicle may join or depart a network frequently, while an appliance in your house is always in its network. Thus, a detector can easily detect two identifications (IDs) of the same value if a faked appliance joins the network. However, in V2G networks, if an adversary vehicle steals a legal vehicle's ID to recharge, when the legal vehicle does not connect to the network, it is very difficult to find out. To address the above problems, various privacy preservation researches have been done aiming at benefiting utility companies and protecting customers at the same time, as well as satisfying its special privacy preservation requirements.

In this paper, we survey papers addressing privacy preservation problems in V2G networks, including location privacy, ID privacy, anonymous authentication, etc. We discuss what types of privacy data these papers aim to protect, where some sensitive information may be leaked in V2G networks, and what kinds of typical privacy attacks there are. To address these questions, we introduce various privacy preservation approaches and analyze the approaches that these papers employ. We further discuss privacy preservation techniques which have already been used in V2G networks and those who have potential applicability. There are already some surveys on Smart Grid privacy preservation, e.g., the paper [19], but this paper is the first survey on privacy preservation for V2G networks, to the best of our knowledge.

The rest of the paper is organized as follows: Section 2 introduces unique features of privacy preservation in V2G networks and various related issues. In Section 3, we introduce privacy preservation approaches and goals. We introduce privacy preservation problems and challenges in Section 4. In Section 5, the current state of the art techniques and research works of privacy preservation in V2G networks are introduced and summarized. We summarize solved problems, related techniques and their pros and cons in Section 6. The unsolved problems and possible solutions are presented in Section 7. Finally, we conclude the paper in Section 8 and present future work.

2. Privacy Issues in V2G Networks

In this section, we will introduce various privacy issues in V2G networks.

2.1. Unique privacy concern

The privacy issue of V2G networks is more complicated than other networks in Smart Grid. In HANs, BANs or IANs, customers or businesses worry about smart meters installed outside their houses or buildings that may potentially leak their sensitive information. In V2G networks, an EV is the customer when it recharges, and it is the service provider when it sells its power back to the grid or to other EVs. As a customer, it does not want its personal information to be leaked out. As a service provider, it does not want its customers to know who provides the service. This unique characteristic raises a great challenge on traditional privacy preservation solutions, and even solutions for other networks of Smart Grid may not be applicable.

2.2. Privacy-sensitive data

To address the privacy preservation problem in V2G networks, the first thing that we need to know is that what types of data or parameters in V2G networks are privacy-sensitive. As shown in Table 1, these are typical data in V2G networks, including customer ID, location, meter reading, etc. Some of these data are related to billing services, such as time and clock. Some of these data are security related, such as configuration data. Some data have privacy impacts. From this table, we can see that there are four types of privacy-sensitive data: ID, location, access control policy, and payment and tariff data.

The paper [20] introduces possible personal information leakage if an EV's location and ID are abused by an adversary. The information about you includes [20]: time that you leave and return home; location of your residence, personal wealth, and financial status; your workplace and possible salary; doctors who you visit, types of the doctors, visiting frequency, and possible health condition; your friends' information and your socioeconomic status; etc.

2.3. Attacks of leaking privacy

There are various attacks in V2G networks, such as replay attack, Denial of Service (DoS) attack, etc., and some of them are privacy preservation related [21].

2.3.1. Eavesdropping

Eavesdropping attack is a passive attack in which an attacker eavesdrops the network to get more information to help active attacks. The adversary can eavesdrop any connection to the network if (s)he has physical or logical access. Personal information included in the messages, such as ID, location, and billing information, could be leaked out.

2.3.2. Man-in-the-Middle attack

An attacker may intercept the connection between the vehicle and the charging spot or the LAG to modify the original message for a malicious purpose. Or the adversary could connect a faked charging spot to the real one, and consume the charging energy partially without paying for it. This attack could expose user's privacy since the message may contain personal information.

2.3.3. Impersonation attack

Impersonation attack is that an adversary forges a legal entity in the network, such as an LAG, an EV, or a charging spot, to obtain the access authority. If an LAG or charging spot cannot discern the suspicious vehicle, the vehicle can get authorized access and steal energy and information. Furthermore, if the vehicle cannot distinguish a compromised LAG or charging spot, its real ID or other information may potentially be exposed. The way to prevent this attack is to hide entities' real IDs, such as using blind signature to hide real IDs from the local LAGs.

Table 1: Typical Data of V2G Networks and their Privacy Impact

Data	Billing relation	Reliability relation	Security relation	Privacy relation	Description
Customer ID			√	√	customer name, vehicle ID
Location data			√	√	charging location and schedule
Meter data	√				electricity consumed or supplied over a time period
Configuration data		√	√		system operational settings, thresholds for alarms, task schedules, policies, etc.
Control commands		√	√		inquiries, alarms, events, and notifications
Access control policies		√	√	√	permitted communication partners, their credentials and roles.
Time, clock setting	√	√	√		used in records and sent to other entities.
Payment and tariff data				√	informing consumers of new or temporary tariffs as a basis for purchase decisions.
Firmware, software, and drivers		√	√		software components installed and may be updated remotely.

2.3.4. Sybil attack

Sybil attack is where an attacker creates a lot of pseudonymous IDs for a malicious purpose. Sybil attack may occur in V2G networks where an EV is allowed to have multiple IDs [22]. A compromised EV may present multiple IDs and function as multiple distinct EVs. The system's vulnerability to Sybil attack depends on the cost of generating IDs.

2.3.5. Physical attack

Physical attack means that an EV, LAG, or charging spot has some tampered or substituted components. This attack normally cannot be detected automatically by security schemes since the embedded software, hardware, or firmware has been replaced, and it is no longer functional correctly. The way to deal with this attack is to perform a routine check on devices periodically.

2.4. Where are privacy data leaked out?

In V2G networks, privacy data may be leaked in different processes or components of the networks.

2.4.1. Charging and discharging

Charging service is one of the most basic functions of V2G networks, where EVs get electricity from the power grid to charge batteries. Discharging is where an EV provides its electricity to the grid or other EVs. During the charging process and the discharging process, EVs have to provide their IDs, plug into charging spots, connect to LAGs, and communicate with service providers. However, the two-way electric flow and continuous monitoring during the two processes potentially expose user's private data, such as locations of charging or discharging [23, 24].

2.4.2. Battery management

Battery management is to manage the battery status of an EV. Vehicles in V2G networks are EVs, which mostly have batteries installed. Battery information can provide additional information for the adversaries to analyze the vehicle owner's movement profile [25]. The charging and discharging processes are related to battery management, but they refer to the interactions between EVs and LAGs.

2.4.3. Communication

The two-way communication is an attracting characteristic of V2G network and is totally different from that in the traditional power grid. However, the two-way communication also facilitates attackers [26]. To attack V2G networks is much easier than to attack the traditional grid. Communication in V2G networks includes various connections, such as the connections between EVs and LAGs, the connections between LAGs and remote operators, etc. All of the connections have risks of privacy exposure.

2.4.4. Data management

Data management in V2G networks includes data collection, aggregation, storage, and publication. Continuous monitoring of the V2G networks could generate a large amount of data. These data contain user's information including IDs, charging strategies, locations, and billing information. To compete with its peers, a utility company may take advantage of customers by analyzing these data and obtaining customer profiles. Curious database administrators may peek on these data. Attackers may show great interests on hacking the database or storage systems. Furthermore, various malicious software and attacks are aiming at database or storage systems. How to process these data under privacy preservation consideration is still a challenge.

2.4.5. Billing and payment

Billing in V2G networks is also different from the traditional power grid. The billing in the traditional power grid is one-way while it is two-way billing in V2G networks. The pros and cons of different payment schemes are discussed and compared in Table 2. Judging Authority (JA) is responsible for investigating disputed transactions. Although credit card can satisfy most of the needs of V2G networks, it is not a good way to protect privacy since in many financial applications, even though credit numbers are encrypted, some information related to credit cards is not encrypted [27]

2.4.6. Protocol vulnerability

V2G networks may employ ISO/IEC 15118 as the charging protocol between EVs and charging spots, adopt IEC 61850 for the communication between charging spots and energy providers, and use Open Charge Control Protocol (OCPP) as the communication protocols between charging spots and mobility operators [3]. There are various other candidate protocols for communication, including IEEE 802.11 family [28], Power Line Communications (PLC) [29], and SAE series [30]. All of these protocols have vulnerabilities. Attackers may make use of the loopholes in these protocols for malicious purposes.

3. Privacy Preservation Goals and Approaches

There are three general approaches to achieve privacy preservation in V2G networks: data minimization, data generalization, and data suppression. Privacy preservation could be divided into anonymity, unlinkability, undetectability, unobservability, and pseudonymity [32].

3.1. Data minimization

As a term in law, data minimization is the practice to eliminate information stored by a(n) business, organization or individual unnecessarily. The purpose is to decrease the risk of possible information leakage and identity theft. Data minimization means that 1) the possibility of collecting personal data about others should be minimized; 2) collected personal data should be minimized within the remaining possibilities of 1); 3) the time to store these collected personal data should be minimized [32].

3.2. Data generalization

Data generalization is the process of generating summary data with successive layers for a dataset. The purpose of data generalization, regarding privacy preservation, is to hide the characteristic of an individual from its group, such that the adversary will not able to distinguish this individual from its peers. For a numerical value, a typical way is to replace the value by a range of it, so that the accuracy of the observation of an adversary decreases. The advantage of using data generalization in V2G networks is that we can enhance privacy including all of the vehicles in services. In the paper [25], the State of Charge (SoC) information of different EVs is generalized. Instead of showing the accurate value of SoC, each EV only shows the range of its SoC, and thus mixes with other EVs falling in the same range.

3.3. Data suppression

In V2G networks, data suppression means selectively not disclosing certain data values of the networks services, the vehicles, the charging services, the devices, or any combination of the above. The papers [33, 31, 34, 35, 36] all employ data suppression approaches to achieve privacy preservation in V2G networks. The method in the paper [31] suppresses IDs of the vehicles to protect payment information, and the method in the paper [35] suppresses ID data to protect location information.

3.4. Anonymity

Anonymity in V2G networks means that a subject, e.g., a vehicle, a device, or a data value, cannot be identified in all possible subjects [37]. In the paper [31], a two-way anonymous payment system is proposed, and with this system, a customer can pay for her/his bill anonymously. More importantly, when the customer sells the electricity of her/his vehicle to the grid, (s)he can also get paid without revealing her/his information. In the paper [35], the authentication process is anonymous when a vehicle joins a network so that an adversary cannot locate the vehicle.

3.5. Unlinkability

Unlinkability in V2G networks means that an adversary cannot sufficiently distinguish whether or not two or more subjects in the networks are related. The paper [33] analyzes interactions in V2G networks, including 1) interactions between vehicles, 2) interactions between a vehicle and a charging station, and 3) interactions between a vehicle and an LAG. They propose an adversary algorithm to illustrate how an adversary can link interactions to obtain unauthorized information.

3.6. Undetectability

Undetectability in V2G networks means that an adversary cannot sufficiently distinguish whether a target, e.g., a vehicle, device or data item, exists or not. To the best of our knowledge, there is no research work focusing on undetectability in V2G networks now. But in other parts of Smart Grid, similar works have been proposed. The paper [38] proposes a power management model for HANs in Smart Grid. This model adopts a rechargeable battery and proposes a recharging algorithm for it, so that an adversary cannot be able to distinguish a load event of an appliance, given a home load signature defined as the sum measured loads of all appliances according to a given formula.

3.7. Unobservability

In V2G networks, unobservability means that an adversary cannot sufficiently distinguish whether a target performed some certain kinds of actions, such as sending a message, receiving a message, or logging in. The relationship between anonymity, unlinkability, undetectability, and unobservability, introduced in the paper [32], states as follows:

Table 2: Comparison of Existing Payment Systems [31]: √ indicates fully supported; × indicates Not supported; ◦ indicates partially supported

Scheme	Location privacy	Prevention of cheating	Support JA	Low implement cost	Lost protect.	2-ways transaction	Stolen car trace
Paper cash	√	√	×	×	×	√	×
Prepaid cashcard Cash coupon	√	√	×	√	×	◦	×
Transferrable e-cash	√	×	◦	√	×	√	×
Credit card	×	√	√	√	√	√	×
Paypal	◦	√	√	√	√	√	×

1. To the same adversary, unobservability always reveals only a partial information what anonymity reveals.
2. To the same adversary, unobservability always reveals only a partial information what undetectability reveals.

3.8. Pseudonymity

In V2G networks, pseudonymity means that an entity uses a pseudonym ID instead of its real name or ID. Pseudonymity in V2G networks is often achieved by ID-based blind signature, which we will introduce in details in later sections. The paper in [39] proposes an architecture that analyzes V2G privacy integrated with Smart Grid infrastructure, and it employs access control profiles to regulate the data flow between gateway and service providers. All information are pseudonymised by the gateway.

As shown in Table 3, the papers we introduced are all privacy preservation related but adopt different approaches.

4. Privacy Preservation Problems and Challenges

In this section, we will introduce various privacy preservation problems and challenges in V2G networks.

4.1. Concealed data aggregation

LAGs collect EVs' data during charging/discharging process and aggregate data to get partial results. The aggregation process shares the workload of head end systems in utilities, and the results help utilities to predict grid load and to schedule transmission. However, privacy related data, such as identity and location, are also collected, which potentially expose customers' sensitive information. Concealed data aggregation is to collect and aggregate data without revealing privacy related data.

4.2. Anonymous authentication

When EVs join V2G networks or send messages, they should be authenticated. The authentication process is to determine that the EVs are who they are declared to be. However, this process potentially exposes customers' personal information [40]. The purpose of anonymous authentication is to authenticate successfully EVs and hide privacy related data at the same time.

4.3. Privacy-preserving billing and payment

When EVs get electricity from the grid, they should pay for it, and when they sell extra electricity back to the grid, they should get paid. The billing and payment systems have to distinguish exactly these EVs and their transactions before real billing and payment execute. However, this process could reveal customers' sensitive information, such as identity and credit card information. Privacy-preserving billing and payment are to design a system which can protect customers' privacy while providing reliable billing and payment function.

4.4. Charging unlinkability

If an EV's charging information is exposed to an adversary, it could be used for a hijack. For example, if an EV charges at location A, an adversary could analyze and predict its next charging spot by using its battery status, charging spot distribution and other information [25]. Charging unlinkability is to mix an EV's charging status with other EVs', thus, to protect customers' privacy.

4.5. Identity privacy

To uniquely identify an EV, each EV has a unique identity in V2G networks. If the identity of an EV is exposed to an adversary, the adversary could utilize this identity to retrieve related personal information. Identity privacy is to prevent identities from leakage.

4.6. Location privacy

An EV can move from place to place. If an EV's location information is exposed to an adversary, the adversary could obtain its movement information and predict its next stop. If location privacy is not well protected, it could be used for a malicious purpose, such as hijacking.

4.7. Privacy-preserving discharging

Discharging means selling electricity to the grid. In V2G networks, EVs can sell extra electricity back to the grid and get paid. Discharging is a new function comparing to the traditional power grid, and it is still under development. Beside guaranteeing the main function of discharging, customers' privacy also concerns with the design process.

Table 3: Privacy-preserving Approaches

Reference	Data protected	Approach	Goal
Kalogridis et al. [38]	Electricity data	Data generalization	Undetectability
Stegelmann et al. [25]	Location	Data generalization	Unlinkability
Stegelmann et al. [39]	ID	Data suppression	Pseudonymity
Yang et al. [35]	ID location access control	Data suppression	Anonymity
Liu et al. [31]	Payment	Data suppression	Anonymity
Liu et al. [34]	ID access control	Data suppression	Unlinkability
Stegelmann et al. [33]	ID	Data suppression	Unlinkability

4.8. Privacy-preserving data publication

Different from traditional monthly bills, customers can access their usage information and statistic reports at any time. Data are published via head end servers, and customers can access these data through apps installed on mobile devices or computers. However, a curious DB (Database) admin might peek into the servers and adversaries might eavesdrop communication channels to obtain customers' sensitive information. We need to design a privacy-preserving data publication scheme to protect customers' privacy.

5. Privacy Preservation Techniques

In this section, we will introduce current state of the art privacy preservation techniques, and survey existing research works in V2G networks based on these techniques.

5.1. Blind signature

Blind signature is mainly adopted by authentication schemes of V2G networks and allows a requester to get a signer's message's signature concealing the message content.

Blind signature can be classified into fully blind signature [46] and partially blind signature [41, 42, 43, 44, 45]. Fully blind signature is that a signer knows nothing about the message. In the partially blind signature algorithm, the signature includes clearly visible and common-agreed information. Some blind signature schemes are restrictive [41, 42, 43], and this means that the message choice needs to follow certain rules and the choice is restricted.

Blind signature can also be classified into certificate (CA)-based blind signature [47] and ID-based blind signature [41, 42, 43, 44, 45]. CA-based blind signature needs a CA to generate key pairs for the entities in the network. ID-based blind signature uses an entity's ID as the public key. Employing blind signature in V2G networks is simple, but the communication overhead will increase if the authentication process is complex.

As shown in Table 4, there are various blind signature algorithms employed in V2G networks. Almost all the existing blind signature schemes adopted in V2G network are ID-based partially restrictive blind signature. The proposed p^2 scheme [35] is based on ID-based restrictive partially blind signature. The basic idea is the blindness property of the permit which keeps EV's real ID unknown to the LAG. Moreover, LAGs will provide an individual EV a precise reward without knowing real ID of the EV.

The paper [31] also discusses location privacy of electric vehicles in V2G networks, but from the aspect of anonymous payment system. The authors analyze all existing payment systems, including paper cash, e-cash, prepaid cash card/cash coupon, Paypal, and credit card. But none of the above achieves location privacy, prevention of cheating, support of Judging Authority (JA), low implementation cost, lost protect, two-way transaction, and stolen car trace at the same time. This payment system employs partially restrictive ID-based blind signature. It hides vehicle's real ID during the recharging payment and rewarding processes at the same time achieving two-way anonymity. This system includes three roles: user (electric vehicles), supplier (utility companies), and judging authority (the third party). The system has two modes: portable mode and embedded mode. In the portable mode, a user uses a single account to manage all his/her vehicles and communicates with V2G networks via portable mobile devices. This mode is convenient for users who want to manage more than one car in one account and easier to manage a car driven by different persons, such as Taxi. In the embedded mode, each vehicle has a unique account, and the hardware device embeds in the vehicle. This system supports tracing stolen cars, only available in the embedded mode. If a car is stolen, the owner could report to the supplier immediately and present the secret number. In this way, the stolen car could be identified. Any charging station receiving this secret number will report to the supplier or police immediately.

5.2. Group signature

Group signature allows each member in a specific group to sign a message on behalf of the group without revealing the member's identity. Group signature provides anonymity and traceability and supports addition and revocation of members. Group signature schemes can be classified into

Table 4: Categories of Blind Signature

Reference	Partially blind signature	Restrictive blind signature	ID-based blind signature
Au et al. [41]	√	√	√
Tseng [42]	√	√	√
Vaidya et al. [43]	√	√	√
Li et al. [44]	√		√
Wang et al. [45]	√	√	√
Yang et al. [35]	√	√	√
Liu et al. [31]	√	√	√

master-based group signature schemes [48] and manager-based group signature schemes [34, 49, 50, 51]. In a master-based group signature scheme, a trusted group master is employed to issue secret keys to its members and publish the related public key in the group. In a manager-based group signature scheme, a group manager is employed to help to issue secret keys but has no knowledge of the keys. Group signature schemes can also be classified into static group signature schemes [48] and dynamic group signature schemes [34, 49, 50, 51]. In a static group signature scheme, the members of a group are predefined and thus no group member can join the group once it initiates. In a dynamic group signature scheme, group members can be added at any time.

Group signature is employed in V2G networks mainly to solve the problem of anonymous authentication. LAGs play the role of masters or managers. A group of EVs is treated as a whole. A recipient of a message signed by an EV in the group cannot learn which EV it is from, thus protecting the EV's privacy. Some recent research works are shown in Table 5. To the best of our knowledge, all group signature schemes adopted in V2G networks are manager-based and dynamic. One benefit is that LAGs cannot access EVs' secret keys, and thus it lowers the possibility of EVs' privacy leakage. Furthermore, to make the schemes more flexible, EVs are allowed to join a specific group at any time.

The paper [34] proposes a privacy-preserving authentication scheme based on aggregated-proofs for V2G networks in Smart Grid. The basic idea is to divide EVs into two working modes: the visiting mode and the home mode. In the home mode, an EV connects to its frequent connected LAG, such as the LAG at the vehicle owner's parking lot at work or residential place. The visiting mode is the mode that an EV from other areas temporarily accesses the LAG. These two modes have different security requirements and need different authentication schemes. The authors in [34] propose a concept of virtual battery vehicle (VBV), which is an independent component attached to an LAG. A VBV acts as a manager in the algorithm based on group signature, which helps in-group authentication. For out-group authentication, a VBV needs CA's justification to communicate with LAGs and other VBVs. Thus, LAGs cannot get to know BVs' private information.

5.3. Ring signature

Similar to group signature, ring signature allows each member of a group to sign a message without revealing the member's identity. The main difference is that there is no master or manager in a ring signature scheme. The group is formed on an ad-hoc basis in a ring signature scheme while the group in a group signature scheme forms by a master or manager who regulates join and revocation operations. A recipient of a ring signature can only learn that this signature is from a member of a ring, but not know the knowledge of which member it is from.

Ring signature is employed in V2G networks also to solve the problem of anonymous authentication. The paper in [52] proposes a role-dependent scheme to protect EVs' privacy when they play different roles in V2G networks. When an EV demands electricity from the grid, it plays the role of a customer. When an EV sells electricity to the grid or supplies electricity to the other EVs directly, it plays the role of a generator. Moreover, when an EV is not in the charging or discharging mode, it plays the role of storage. The scheme in [52] employs ring signature to authenticate EVs playing roles of customers. A group of EVs forms a ring. An LAG can only learn general attributes of the group. The LAG and other adversaries are not able to reveal an EV's real identity and its location information.

5.4. Secret sharing

Secret sharing is where a secret divides into several parts, and each part is held by a participant. To restore the secret, all or at least some of the parts are required. Secret sharing is employed in V2G networks mainly to solve the problem of anonymous data aggregation.

In the paper [53], Shamir Secret Sharing (SSS) scheme is employed to build a privacy-preserving V2G infrastructure. Three types of data are split into parts. They are EVs' plug in time periods, EVs' current charge level of the batteries, and the amount of recharged electricity. Each one in a set of LAGs holds one part of the data. Furthermore, these LAGs work collaboratively during the EVs' charging or discharging process. Since a single LAG only learns a part of an EV's attributes, the EV's privacy will not be leaked out if the LAG is compromised. In the proposed infrastructure, all parts are required to reconstruct the information. EVs' privacy protection is guaranteed since the possibility that all LAGs are compromised at the

Table 5: Categories of Group Signature

Reference	Manager-based group signature	Static group signature
Liu et al. [34]	√	√
Liu et al. [49]	√	√
Chen et al. [50]	√	√
He et al. [51]	√	√

same time is very small and therefore we assume that the probability is zero.

5.5. Homomorphic encryption

Homomorphic encryption is mainly used in data aggregation of V2G networks. Homomorphic encryption allows binary operations, such as addition and multiplication, on encrypted data directly, without the need of decrypting it in advance [54, 55].

There are various homomorphic encryption methods, as shown in Table 6, and they can be classified into fully homomorphic encryption and partially homomorphic encryption [60, 56, 57, 58, 59, 54, 55]. Fully homomorphic encryption supports both "addition" and "multiplication" operations. Partially homomorphic encryption schemes exclusively support either addition or multiplication, but not both. All of the methods used in V2G networks so far, even in Smart Grid, are partially homomorphic encryption. Homomorphic encryption methods can also be classified into symmetric homomorphic encryption [60, 56, 57] and asymmetric homomorphic encryption [58, 59]. Symmetric homomorphic encryption uses symmetric keys while asymmetric homomorphic encryption uses asymmetric keys.

Homomorphic encryption is an effective method for data aggregation in V2G networks. Since the data aggregation in V2G networks only needs additive operations, partially homomorphic encryption is enough to satisfy the privacy preservation requirement in V2G networks and the computational overhead is not large. Transactions in V2G networks often take half an hour to several hours [61], and thus it allows a lot of time for homomorphic encryption module to finish its work in time.

A privacy-preserving architecture for V2G networks, called IP^{2}DM, was proposed in [60]. In this architecture, data are encrypted like an onion, and each layer represents a different encryption algorithm. The benefit of onion-level encryption is that it can build different "onions" for different applications to meet different security requirements. The HOM (Homomorphic) layer is homomorphic encryption layer. A practical system as a case study where the HOM layer employs a hierarchical partial blind signature [54] was implemented. LAGs collect data from EVs and aggregate to get partial results. The center server collects data from LAGs and performs global aggregation. Another homomorphic encryption algorithm in the paper [55] can also be adopted by the HOM layer to achieve anonymous data aggregation.

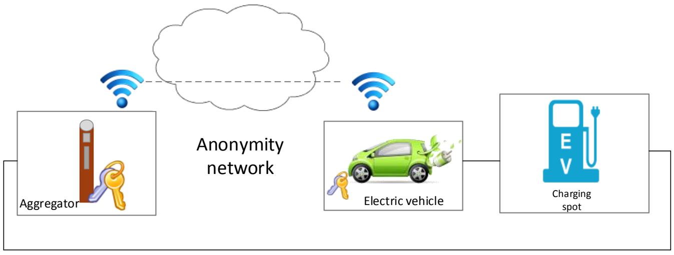

Figure 3: Privacy-preserving interaction architecture based on anonymity networks in V2G networks [33].

Some homomorphic encryption schemes [56, 57, 58, 59] proposed for Smart Grid fit into the context of V2G networks [61].

5.6. Third-party anonymity

Another typical method to protect privacy in V2G networks is third-party anonymity, which employs one or multiple tamper-resistant devices to hide an entity's sensitive information.

The paper [62] proposes a privacy-preserving roaming charging protocol for V2G networks. A tamper-resistant hardware, smart card, is issued by a service provider and attached to an EV. The smart card stores certificate and user's secret keys. A roaming EV sends a charging request via the smart card using pseudonym to hide its real ID. Each charging session of the same EV uses a different pseudonym, and thus an adversary is not able to link different charging sessions of the same EV. The paper [63] proposes a designing privacy-preserving scheme for EVs which act as energy storage. It also introduces a tamper-resistant device attached to an EV. A charging/discharging request is sent via the device using pseudonym as well. Different from the scheme in the paper [62], a different pseudonym is used only when the EV moves from on station to another.

5.7. Anonymity Networks

Anonymity networks are a class of communication networks, which employ Certificate Center and Public Key Infrastructure to hide the network layer IDs in V2G networks. The architecture is shown in Fig. 3.

Anonymity networks once were thought to be able to achieve the privacy preservation purpose [11]. However, the paper [33] proposes an adversary algorithm to show that an adversary can still distinguish an individual vehicle from its peers in an anonymity network. The authors [33]

Table 6: Categories of Homomorphic Encryption

Reference	Partially homomorphic	Symmetric homomorphic	Asymmetric homomorphic
Wang et al. [56]	√	√	
Mármol et al. [57]	√	√	
Lu et al. [58]	√		√
Li et al. [59]	√		√
Han et al. [60]	√		√

find that an adversary can improve his/her ability to link distinct V2G instances by combining information observed at charging stations and other constraints. They mathematically model the behaviors of an adversary and present an adversary algorithm to support their claim. By this algorithm, the adversary can determine whether two different interactions are from the same vehicle without knowing their exact IDs. A simple example is presented to show how the algorithm works, and the authors also model the adversary's knowledge in the form of a bipartite graph [33].

6. Solved Problems and Discussion

Upon now, we have discussed various problems and techniques. We summarize problems solved and related techniques, shown in Table 7. Here, we define "solved" as "a solution exists in V2G networks related literature". "Solved" does not mean "perfectly solved." We will also discuss the pros and cons of each technique that used to solve a problem.

As shown in Table 7, the problems that we believe solved, at least partially solved, include concealed data aggregation, anonymous authentication, privacy-preserving payment and billing, charging unlinkability, identity privacy, and location privacy. The references and techniques overlap on some problems since a scheme or technique proposed in a reference could solve multiple problems.

6.1. Concealed data aggregation

Techniques used to solve the problem of concealed data aggregation in V2G networks include homomorphic encryption and secret sharing. Both of these two techniques can address this problem, and however they both have some drawbacks. The drawback of homomorphic encryption is that it is vulnerable to physical attacks or impersonation attacks on LAGs. In the scheme proposed in the paper [56], which is based on symmetric homomorphic encryption, its symmetric key will be exposed to an adversary if an LAG is compromised. Then the adversary could reveal the real values of EVs' data using the symmetric key. In the scheme [58] based on asymmetric homomorphic encryption, the real values of EVs' data and their private keys can keep confidential if an LAG is compromised. However, the adversary could still falsify aggregation results using the public keys, and send these fake results to the head end. On the contrary, the scheme [53] based on secret sharing is resistant to physical attacks or impersonation attacks on LAGs, since an LAG only learns a part of an EV's attributes.

The drawback of secret sharing is that the communication overhead is large. A set of LAGs work collaboratively during an EV's charging/discharging process, therefore each LAG and the EV have to communicate with each other simultaneously. By contrast, an EV only needs to communicate with one LAG and the LAG does not need to communicate with other LAGs, if using homomorphic encryption.

6.2. Anonymous authentication

Techniques used to solve the problem of anonymous authentication in V2G networks include blind signature, group signature, and ring signature. All the works based on any of the three techniques that we surveyed in this paper can achieve anonymous authentication. However, they have pros and cons when comparing to each other. The con of employing blind signature is large communication overhead comparing to group signature and ring signature. All EVs have to authenticate to the head end. On the contrary, the authentication workload is shouldered by in-group members in a group signature based scheme [34] or in a ring signature based scheme [52]. If comparing the communication overhead between group signature and ring signature, the later one has a larger communication overhead since members in a ring communicate on an adhoc basis.

The cons of employing group signature and ring signature is the strength of anonymity. The strength of anonymity of group signature and ring signature is decided by the number of members in a group or a ring. Extremely, if there is only one member in a group or a ring, this member is not anonymous. If we have to compare the security performance of group signature and ring signature, the former one suffers to attacks on the master or manager of a group.

6.3. Privacy-preserving billing and payment

Blind signature is the technique employed to design privacy-preserving billing and payment systems for V2G networks. The schemes proposed in the papers [41, 31] are both based on ID-based partial restrictive blind signature, which provides unconditional anonymity. Unconditional anonymity guarantees that all transactions are executed absolute anonymously. The advantage is that the schemes

Table 7: Solved Problems and Employed Techniques

Problem	Technique	Pro	Con	Reference
concealed data aggregation	homomorphic encryption	low communication overhead	vulnerable to attacks on LAGs; low computational overhead	[56, 57, 58, 59, 60]
	secret sharing	resist to attacks on LAGs; high computational overhead	high communication overhead	[53]
anonymous authentication	blind signature	highly anonymous	high communication overhead	[41, 42, 43, 44, 45, 35, 31]
	group signature	low communication overhead	vulnerable to attacks on manager nodes	[34, 49, 50, 51]
	ring signature	resist to attacks on manager nodes	anonymity strength relies on the number of nodes in a group	[52]
privacy-preserving billing and payment	blind signature	highly anonymous	could be used for crimes	[41, 31]
charging unlinkability	third party anonymity	hardware level security performance	extra device and maintenance cost	[62, 63]
	group signature	cost-effective	relatively weaker security performance	[49, 51]
identity privacy	ID-based blind signature	highly anonymous	high communication overhead	[41, 42, 43, 44, 45, 35]
	third party anonymity	hardware level security performance	extra device and maintenance cost	[62, 63]
	group signature	low communication overhead and cost-effective	vulnerable to attacks on manager nodes	[34, 49, 50, 51]
	ring signature	resist to attacks on manager nodes and cost-effective	anonymity strength relies on the number of nodes in a group	[52]
location privacy	blind signature	highly anonymous	high communication overhead	[31, 41, 42, 43, 44, 45, 35]
	third party anonymity	hardware level security performance	extra device and maintenance cost	[62, 63]
	group signature	low communication overhead and cost-effective	vulnerable to attacks on manager nodes	[34, 49, 50, 51]
	ring signature	resist to attacks on manager nodes and cost-effective	anonymity strength relies on the number of nodes in a group	[52]

can protect customers' privacy very well. However, the unconditional anonymity could be utilized for crimes, such as blackmailing and money laundry. When police invest a blackmailing case, they may find that they cannot reveal the real ID of the suspect who received the money via an unconditional anonymous payment system.

6.4. Charging unlinkability

Techniques used to solve the problem of charging unlinkability include third party anonymity and group signature. Third party anonymity [62] provides hardware level encryption and anonymity, and it has better security performance than software level encryption. However, it requires extra devices and thus it is more expensive. Moreover, a utility has to maintain a large number of certificates if using third party anonymity, which also raises potential costs. Comparing to third party anonymity, group signature is more flexible and cost-effective.

6.5. Identity and location privacy

The techniques employed to address the problems of identity privacy and location privacy overlap with the techniques of anonymous authentication, charging unlinkability, and privacy-preserving billing and payment, and as do the references. The reason is that these papers [41, 42, 43, 44, 45, 35, 34, 49, 50, 51, 52, 62, 63] all hide an EV's real ID, though, based on different techniques, thus providing anonymity and unlinkability. Moreover, location privacy problem is indirectly solved by hiding the IDs in the papers [41, 42, 43, 44, 45, 35, 34, 49, 50, 51, 52, 62, 63]. The paper [31] addressed location privacy problem by hiding an EV's location directly. However, it cannot address identity privacy problem at the same time.

7. Unsolved Problems and Techniques Need Further Research

In this section, we will summarize unsolved privacy preservations problems in V2G networks among these papers surveyed. Here, we define "unsolved" as "did not find a proposed solution in existing literature related to V2G networks". There might be some solutions proposed for similar problems in other fields. We will further study their applicability in V2G networks.

As shown in Table 8, we list two problems that the surveyed papers did not address, including privacy-preserving discharging and privacy-preserving data publication.

7.1. Privacy-preserving discharging

Privacy-preserving discharging is an open issue in V2G networks. Although there are several research works addressing charging problems [62, 63, 49, 51], none of them carries out a solution for discharging problems. Privacy-preserving discharging is one of the future works.

7.2. Privacy-preserving data publication

Privacy-preserving data publication is an open issue which we are working on. Data publication in V2G networks means service providers store and publish users' data online, including charging, discharging, billing, payment, etc., so that users can access their data and search for statistic reports. To the best of our knowledge, there are no research works addressed this problem in current literature in V2G networks. We proposed IP^{2}DM [60] architecture aiming at addressing privacy-preserving data management. The anonymous data aggregation part is already finished and fully presented in the paper, together with the overview of data publication techniques. We will introduce possible techniques which could solve the problem of privacy-preserving data publication in the following subsections.

7.2.1. Encrypted keyword search

Encrypted keyword search allows SQL operations, such as = and LIKE, directly executed on encrypted data. A user can search via a web page interface or other search engines without revealing the keywords (s)he searches with. This technique can be adopted for V2G networks data publication, supporting user queries, such as "how many kWh of electricity did my household use this month?".

Encrypted keyword search can be classified into single-keyword search [64, 65] and multiple-keyword search [66]. In single-keyword search, there is only one keyword, while there are multiple keywords in multiple-keyword search. The paper [64] studies the need of search capability authorization, which can reduce the privacy exposure due to searching and establish a scalable Authorized Private Keyword Search (APKS) framework for encrypted data for Cloud. Two solutions for APKS are proposed using Hierarchical Predicate Encryption (HPE), and online Personal Health Record (PHR) is used as a case effective study.

Encrypted keyword search can also be classified into precise-keyword search [64, 66] and fuzzy-keyword search [65]. The paper [66] proposes choosing the efficient principle of "coordinate matching" to provide multi-keyword ranked search for encrypted data. In other words, as many matches as possible. "Coordinate matching" first captures the similarity between data documents and search query, and then employs "inner product similarity" for similarity measurement to quantitatively formalize such principle.

Moreover, encrypted keyword search can also be classified into single-user encrypted search and multi-user encrypted search [67, 68]. In the paper [67], a Multi-User relational Encrypted DataBase (MuteDB), is proposed to provide confidentiality by executing SQL operations on encrypted data. MuteDB is designed for Cloud database where multiple geographically different users can access the database simultaneously.

A future work is to study the best algorithm among the above and others for V2G networks.

Table 8: Unsolved Problems and Techniques Need Further Research

Problem	Technique needs further research	Reference
privacy-preserving data publication	Search on encrypted data	[64, 65, 66, 67, 68]
	Order-preserving encryption	[61, 69, 70]
Privacy-preserving discharging	future research	

7.2.2. Order-preserving encryption

Order-preserving encryption allows order-related SQL operations, such as ORDER BY, SORT, MIN, and MAX, executed directly on encrypted data items. By using order-preserving encryption methods, sensitive information, such as the ranks of data, can be kept unrevealed during the data publishing process. This technique can be employed by V2G networks, supporting user queries, such as "In which month, my household electricity bill is the highest?". In our previous work [61], we study the possibility of adopting the scheme proposed in the paper [69] for data publication in V2G networks. This algorithm fits in adjustable encryption employed in [61]. The paper [70] proposes an ideal-secure order-preserving encryption scheme claiming much lower cost and compatible with adjustable encryption. Applying this scheme and other feasible schemes to V2G networks deserves future studies.

8. Conclusion

In this paper, we introduced state-of-the-art research works focusing on privacy preservation issues in V2G networks. These surveyed papers addressed various privacy preservation problems, including ID and location privacy, anonymous billing and payment system, anonymous authentication, and concealed data aggregation. We analyzed the papers and presented their basic ideas and main contributions. These papers employ different kinds of privacy preservation approaches and techniques, address problems in different processes of V2G networks, and protect different types of privacy-sensitive data. We summarized solved problems, techniques used and their pros and cons. We introduced unsolved problems and possible solutions. As a future work, we will further address issues left in the solved problems and study the applicability of possible solutions to those unsolved problems.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China (NSFC) under the grant no. 61374200 and the US National Science Foundation (NSF) under the grant no. CNS-1059265.

References

[1] U. D. of Energy, The smart grid: an introduction, available at: http://energy.gov/oe/downloads/smart-grid-introduction-0, accessed: 02/09/2016.

[2] J. Gao, Y. Xiao, J. Liu, W. Liang, , C. L. P. Chen, A survey of communication/networking in smart grids, Future Generation Computer Systems 28 (2) (2012) 391–404.

[3] R. Falk, S. Fries, Securely connecting electric vehicles to the smart grid, International Journal On Advances in Internet Technology 6 (2013) 57–67.

[4] J. Liu, Y. Xiao, J. Gao, Achieving accountability in smart grids, IEEE Systems Journal 8 (2) (2014) 493–508.

[5] Z. Xiao, Y. Xiao, D. Du, Non-repudiation in neighborhood area networks for smart grid, IEEE Communications Magazine 51 (1) (2013) 18–26.

[6] Z. Xiao, Y. Xiao, D. Du, Exploring malicious meter inspection in neighborhood area smart grids, IEEE Transactions on Smart Grid 4 (1) (2013) 214–226.

[7] W. Han, Y. Xiao, NFD: A practical scheme to detect non-technical loss fraud in smart grid, in: Proceedings of the 50th International Conference on Communications (ICC'14), 2014, pp. 605–609.

[8] W. Han, Y. Xiao, FNFD: A fast scheme to detect and verify non-technical loss fraud in smart grid, International Workshop on Traffic Measurements for Cybersecurity (WTMC'16), accepted, DOI: http://dx.doi.org/10.1145/2903185.2903188 (2016).

[9] J. Mu, W. Song, W. Wang, , B. Zhang, Self-healing hierarchical architecture for zigbee network in smart grid application, International Journal of Sensor Networks 17 (2) (2015) 130–137.

[10] Belmont report, available at: http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html, accessed: 02/09/2016.

[11] H. Chen, Y. Xiao, X. Hong, F. Hu, J. Xie, A survey of anonymity in wireless communication systems, Security and Communication Networks 2 (5) (2009) 427–444.

[12] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, Enabling personalized search over encrypted outsourced data with efficiency improvement, IEEE Transactions on Parallel and Distributed Systems DOI: 10.1109/TPDS.2015.2506573.

[13] Z. Xia, X. Wang, X. Sun, Q. Wang, A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data, IEEE Transactions on Parallel and Distributed Systems 27 (2015) 340–352.

[14] Anti smart meter protesters disrupt smart grid conference, available at: http://stopsmartmeters.org/2013/03/22/anti-smart-meter-protesters-disrupt-smart-grid-conference, accessed: 02/09/2016.

[15] Residents protesting smart grid pilot in worcester, available at: http://www.golocalworcester.com/news/residents-protesting-smart-grid-pilot-in-worcester, accessed: 02/09/2016.

[16] available at: http://mygermantravels.com/2011/05/german-designer-power-masts, accessed: 02/09/2016.

[17] Stop Smart Meters Organization, http://stopsmartmeters.org/, accessed: 02/09/2016.

[18] P. Jokar, N. Arianpoo, V. C. M. Leung, A survey on security issues in smart grids, Security and Communication Networks 9 (3) (2016) 262–273.

[19] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, Cyber security and privacy issues in smart grids, IEEE Communications Surveys & Tutorials 14 (4) (2012) 981–997.

[20] D. P. Ghosh, R. J. Thomas, S. B. Wicker, A privacy-aware design for the vehicle-to-grid framework, in: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS), Wailea, USA, 2013, pp. 2283–2291.

[21] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos,

K. Butler-Purry, Towards modelling the impact of cyber attacks on a smart grid, International Journal of Security and Networks 6 (1) (2011) 2 – 13.

[22] H. Nicanfaryz, P. TalebiFardy, S. Hosseininezhad, V. C. Leungy, M. Dammz, Security and privacy of electric vehicles in the smart grid context: Problem and solution, in: Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications (DIVANet'13), Barcelona, Spain, 2013, pp. 45–54.

[23] M. A. Mustafa, N. Zhang, G. Kalogridis, Z. Fan, Smart electric vehicle charging: Security analysis, in: Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, USA, 2013, pp. 1–6.

[24] L. Langer, F. Skopik, G. Kienesberger, Q. Li, Privacy issues of smart e-mobility, in: Proceedings of the 39th Annual Conference of the IEEE Industrial Electronics Society (IECON'13), Vienna, 2013, pp. 6682–6687.

[25] M. Stegelmann, D. Kesdogan, Location privacy for vehicle-to-grid interaction through battery management, in: Proceedings of the Ninth International Conference on Information Technology: New Generations (ITNG), Las Vegas, USA, 2012, pp. 373–378.

[26] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. Yang, M. Guizani, Securing vehicle-to-grid communications in the smart grid, IEEE Wireless Communications 20 (6) (2013) 66–73.

[27] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, H. Deng, A survey of cyber crimes, (Wiley Journal of) Security and Communication Networks 5 (2012) 422437.

[28] Y. Xiao, Performance analysis of priority schemes for ieee 802.11 and ieee 802.11e wireless lans, IEEE Transactions on Wireless Communications 4 (4) (2005) 1506–1515.

[29] C. Jouvray, G. Pellischek, M. Tiguercha, Impact of a smart grid to the electric vehicle ecosystem from a privacy and security perspective, in: Proceedings of the 2013 World Electric Vehicle Symposium and Exhibition (EVS27), Barcelona, 2013, pp. 1–10.

[30] available at: http://www.sae.org/smartgrid/, accessed: 02/09/2016.

[31] J. K. Liu, M. H. Au, W. Susilo, J. Zhou, Enhancing location privacy for electric vehicles (at the right time), in: Proceedings of the 17th European Symposium on Research in Computer Security, Pisa, Italy, 2012, pp. 397–414.

[32] A. Pfitzmann, M. Hansen, A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, available at: http://dud.inf.tu-dresden.de/Anon Terminology.shtml, accessed: 02/09/2016.

[33] M. Stegelmann, D. Kesdogan, Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction, in: Proceedings of the 8th European conference on Public Key Infrastructures, Services, and Applications (EuroPKI'11), Leuven, Belgium, 2011, pp. 75–90.

[34] H. Liu, H. Ning, Y. Zhang, L. T. Yang, Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid, IEEE Transactions on Smart Grid 2 (2012) 1722–1733.

[35] Z. Yang, S. Yu, W. Lou, C. Liu, p^2: Privacy-preserving communication and precise reward architecture for v2g networks in smart grid, IEEE Transactions on Smart Grid 2 (2011) 675–685.

[36] F. Li, B. Luo, P. Liu, Secure and privacy-preserving information aggregation for smart grids, International Journal of Security and Networks 6 (2011) 28 – 39.

[37] G. Kalogridis, S. Denic, T. Lewis, R. Cepeda, Privacy protection system and metrics for hiding electrical events, International Journal of Security and Networks 6 (2011) 14 – 27.

[38] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, R. Cepeda, Privacy for smart meters: Towards undetectable appliance load signatures, in: Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, 2010, pp. 232–237.

[39] M. Stegelmann, D. Kesdogan, V2GPriv: vehicle-to-grid privacy in the smart grid, in: Proceedings of the 4th International Symposium (CSS'12), Melbourne, Australia, 2012, pp. 93–107.

[40] P. Guo, J. Wang, B. Li, S. Lee, A variable threshold-value authentication architecture for wireless mesh networks, Journal of Internet Technology 15 (2014) 929–936.

[41] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, J. Zhou, A new payment system for enhancing location privacy of electric vehicles, IEEE Transactions on Vehicular Technology 63 (1) (2014) 3–18.

[42] H.-R. Tseng, A secure and privacy-preserving communication protocol for v2g networks, in: Proceedings of 2012 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 2012, pp. 2706–2711.

[43] B. Vaidya, D. Makrakis, H. T. Mouftah, Security and privacy-preserving mechanism for aggregator based vehicle-to-grid network, in: Proceedings of 2012 IEEE Wireless Communications and Networking Conference (WCNC), Rhodes, Greece, 2014, pp. 75–78.

[44] H. Li, G. Dán, K. Nahrstedt, Lynx: Authenticated anonymous real-time reporting of electric vehicle information, in: Proceedings of the 6th IEEE International Conference on Smart Grid Communications (SmartGridComm'15), Miami, USA, 2015, pp. 75–78.

[45] H. Wang, B. Qin, Q. Wu, L. Xu, J. Domingo-Ferrer, TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids, IEEE Transactions on Information Forensics and Security 10 (11) (2015) 2340–2340.

[46] D. Chaum, Blind signatures for untraceable payments, in: Advances in Cryptology-Crypto'82, 1982, pp. 199–203.

[47] X. Chen, F. Zhang, S. Liu, Id-based restrictive partially blind signatures and applications, Journal of Systems and Software 80 (2) (2007) 164–171.

[48] A. Agarwal, R. Saraswat, A survey of group signature technique, its applications and attacks, International Journal of Engineering and Innovative Technology (IJEIT) 2 (10) (2013) 28–35.

[49] H. Liu, H. Ning, Y. Zhang, M. Guizani, Battery status-aware authentication scheme for v2g networks in smart grid, IEEE Transactions on Smart Grid 4 (1) (2013) 99–110.

[50] J. Chen, Y. Zhang, W. Su, An anonymous authentication scheme for plugin electric vehicles joining to charging/discharging station in vehicle-to-grid (v2g) networks, China Communications 12 (3) (2015) 9–19.

[51] M. He, K. Zhang, X. Shen, PMQC: A privacy-preserving multi-quality charging scheme in v2g network, in: Proceedings of 2014 IEEE Global Communications Conference (GLOBECOM'14), Austin, USA, 2014, pp. 675–680.

[52] H. Liu, H. Ning, Y. Zhang, Q. Xiong, L. T. Yang, Role-dependent privacy preservation for secure v2g networks in the smart grid, IEEE Transactions on Information Forensics and Security 9 (2) (2014) 208–220.

[53] C. Rottondi, S. Fontana, G. Verticale, Enabling privacy in vehicle-to-grid interactions for battery recharging, Energies 7 (5) (2014) 2780–2798.

[54] S. Ozdemir, Y. Xiao, Integrity protecting hierarchical concealed data aggregation for wireless sensor networks, Computer Networks 55 (8) (2011) 1735–1746.

[55] S. Ozdemir, M. Peng, Y. Xiao, PRDA: Polynomial regression based privacy preserving data aggregation for wireless sensor networks, Wireless Communications and Mobile Computing 15 (4) (2015) 615–628.

[56] Z.Wang, G. Zheng, Residential appliances identification and monitoring by a nonintrusive method, IEEE Transactions on Smart Grid 3 (2012) 80–92.

[57] F. G. Mármol, C. Sorge, O. Ugus, G. M. Pérez, Do not snoop my habits: Preserving privacy in the smart grid, IEEE Communication Magazine 50 (2012) 166–172.

[58] R. Lu, X. Liang, X. Li, X. Lin, X. Shen, EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications, IEEE Transaction on Parallel and Distributed Systems 22 (2012) 1621–1631.

[59] F. Li, B. Lu, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, in: Proceedings of the

First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, 2010, pp. 327–332.

[60] W. Han, Y. Xiao, IP^{2}DM for v2g networks in smart grid, in: Proceedings of the 2015 IEEE International Conference on Communications (ICC'15), London, UK, 2015, pp. 782–787.

[61] W. Han, Y. Xiao, IP^{2}DM: Integrated privacy-preserving data management architecture for smart grid v2g networks, submitted to a journal (2015).

[62] M. A. Mustafa, N. Zhang, G. Kalogridis, Z. Fan, Roaming electric vehicle charging and billing: an anonymous multi-user protocol, in: Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, 2014, pp. 939–945.

[63] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, V. C. Leung, Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations, in: Proceedings of the 2013 IEEE INFOCOM Workshop on Communications and Control for Smart Energy Systems, Turin, 2013, pp. 3429–3434.

[64] M. Li, S. Yu, N. Cao, W. Lou, Authorized private keyword search over encrypted data in cloud computing, in: Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS'11), 2011, pp. 383–392.

[65] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, W. Lou, Fuzzy keyword search over encrypted data in cloud computing, in: Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM'10), San Diego, USA, 2010, pp. 1–5.

[66] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, Privacy-preserving multi-keyword ranked search over encrypted cloud data, in: Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM'11), Shanghai, China, 2011, pp. 829–837.

[67] Ferretti, Luca, F. Pierazzi, M. Colajanni, M. Marchetti, Scalable architecture for multi-user encrypted sql operations on cloud database services, IEEE Transactions on Cloud Computing 1 (4) (2014) 448–458.

[68] Asghar, M. Rizwan, G. Russello, B. Crispo, M. Ion, Supporting complex queries and access policies for multi-user encrypted databases, in: Proceedings of the 2013 ACM workshop on Cloud computing security workshop (CCSW'13), 2013, pp. 77–88.

[69] A. Boldyreva, N. Chenette, Y. Lee, A. O'Neill, Order-preserving symmetric encryption, in: Proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Cologne, Germany, 2009, pp. 224–241.

[70] F. Kerschbaum, A. Schroepfer, Optimal average-complexity ideal-security order-preserving encryption, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS'14), Scottsdale, USA, 2014, pp. 275–286.