Accepted from Open Call

Network Security and Privacy Challenges in Smart Vehicle-to-Grid

Neetesh Saxena, Santiago Grijalva, Victor Chukwuka, and Athanasios V. Vasilakos

Abstract

Smart vehicle-to-grid (V2G) involves intelligent charge and discharge decisions based on user operational energy requirements, such as desired levels of charging and waiting time. V2G is also supported by information management capabilities enabled by a secure network, such as a reliable privacy-preserving payment system. In this article, we describe the network security and privacy requirements and challenges of V2G applications. We present a new network security architecture to support V2G. We propose a scheme with the following security and privacy-preserving features: anonymous authentication, fine-grained access control, anonymous signatures, information confidentiality, message integrity, remote attestation, and a payment system. This article is oriented toward practitioners interested in designing and implementing secure and privacy-preserving networks for smart V2G applications.

Introduction

Reductions in the cost of energy storage technologies coupled with increased investment in charging stations promise broader deployment of electric vehicles (EVs) around the world. Vehicle-to-grid (V2G) exemplifies an integration of the electric grid with transportation systems. While the main goal of connecting the vehicle to the electric grid is to charge the vehicle, the electric vehicle can optionally inject power into the grid and provide ancillary grid services including demand (load) balancing, frequency regulation, and back-up power. In this article, we discuss V2G network security and privacy requirements and challenges. Electric vehicles are a very flexible resource; they can deliver a small portion of their batteries' energy back to the grid (discharging) when the vehicle is stationary, which is about 22 to 23 hours per day.

Several parties have significant interest in exploring the possibilities of V2G operations. These parties are the vehicle manufacturer, the vehicle battery supplier, the vehicle owner, the electric vehicle supply equipment (EVSE) owner, business/home users, the aggregation service provider, and the electrical utility. V2G also has important applications in military systems, where its integration at military installations can be used as a source for emergency power supply. Additionally, regulatory and governmental agencies also have particular motivations for investigating V2G. It is expected that the development and integration of V2G will increase market penetration for plug-in electric vehicles (PEVs) and renewable energy technologies. V2G can provide electricity operating reserves and assist the utility during times of peak demand and provide cost savings, as currently meeting the demands of peak power is a very expensive obligation for utilities. For these reasons, most electric vehicle manufacturers are currently investigating V2G applications.

V2G communication systems are different from other existing communication systems in several ways, such as vehicle mobility, geographic location of the vehicle, charge and discharge operations, driving pattern, and limited communication range. In terms of security, authentication in the V2G network needs to be fast and efficient in order to support a large number of EVs expected to participate in dynamic charging/discharging. Confidential information, such as vehicle identity, vehicle type, charging and discharging time, and charging station identity (CSID), needs to be protected.

Electric vehicles can communicate with the smart grid via distributed and/or centralized V2G networks for charging/discharging their batteries from/to the grid. To support V2G communications, a Dedicated Short Range Communication (DSRC) protocol is specifically designed for communications-based active safety applications, such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) that includes IEEE 802.11p and IEEE 1609 wireless access in vehicular environments (WAVE) [1]. DSRC provides the communication between the vehicles and electric power systems. V2G systems need a tightly controlled spectrum for highly reliable communications. For instance, WiFi is not a preferred technology in V2G systems, as it can take multiple seconds to recognize nearby stations and complete the association. Active safety applications, such as V2G, V2I, and V2V, require immediate and extremely fast communication establishment with response times in milliseconds in which vehicles and devices must recognize each other and transmit messages to each other. Hence, DSRC is preferred as a communication medium for communications-based active safety systems because it supports high speed, low latency, and short-range

Neetesh Saxena, Santiago Grijalva, and Victor Chukwuka are with Georgia Institute of Technology.

Athanasios V. Vasilakos is with Lulea University of Technology.

Digital Object Identifier: 10.1109/MWC.2016.1600039WC

wireless communication. In addition, DSRC also provides fast network acquisition, secure wireless interface, safety message authentication, high reliability, interoperability, immune performance in extreme weather conditions (e.g., rain, fog, snow, etc.), and supports high-speed vehicle mobility [2].

Unlike traditional payment systems that accept debit/credit cards operated by third parties, thus incurring high processing times, V2G systems have stricter financial transactions requirements. V2G systems require very fast, secure (through cryptographic primitives with an advance amount in the vehicle owner's account at the utility, similar to [3]) and efficient payment system with low processing times in order to accommodate charging and discharging transactions by a large number of vehicles in the network. With large amounts of frequent transactions, a payment solution must also provide anonymity while preserving vehicle owner privacy. A V2G communications network is different from other traditional networks because information exchanges over the V2G network controls physical components in the electric distribution grid. As a result, information or network security breaches may cause the malfunction and/or damage of critical power infrastructure.

There exist security and privacy challenges in the V2G system that can significantly affect the practical use of this next generation technology. The information shared by the EVs and other V2G entities, such as the local aggregator (LAG), communication and authentication servers, billing center, and control center (CC), must be secured over the network. Privacy of personal and confidential information must be maintained. According to IEC 15118-2 [4], the use of transport layer security (TLS) and unilateral authentication (server side authentication) are mandatory. However, mutual authentication (both server and vehicle authentication) is optional. Unilateral authentication is not considered secure, as it may result in redirection and impersonation attacks. It is risky to assume that all the LAGs and/or servers are trusted entities. We strongly emphasize that future generation V2G systems must provide mutual authentication between all vehicles and their respective LAGs or servers in order to ensure that communication happens only among legitimate entities in the network. Furthermore, since information misuse can lead to insider attacks, the LAG must not be able to recognize and/or keep track of any EV by its information and behavioral pattern.

The existing protocols/schemes do not discuss some of the possible attacks in the V2G network, such as man-in-the-middle (MITM), replay, impersonation, redirection, flood-based denial of service (DoS), known key, and repudiation attacks. Since a large number of entities would be involved in future V2G networks, the generated overheads must be kept as low as possible. These overheads have direct impact on the optimal performance-security trade-off [1].

V2G Network Security and Privacy Scenarios

Let us illustrate network security for V2G applications by using an example. Many different entities participate in the V2G network, including the owner of the vehicle, the vehicle battery, the power company, and the payment management company. As illustrated in Fig. 1, the vehicles in the V2G network communicate with the smart grid through a collector or data aggregator for charging their batteries at the charging stations. A data aggregator is an intelligent device or set of devices that acts as a collector of available vehicles' power during discharging, and offers power supply to the vehicles through the charging stations. Aggregators have access to the authentication and communication servers in order to coordinate the charging. We now describe V2G security from the perspective of the various entities.

A data aggregator is an intelligent device or set of devices that acts as a collector of available vehicles' power during discharging, and offers power supply to the vehicles through the charging stations. Aggregators have access to the authentication and communication servers in order to coordinate the charging.

Vehicle Owner Perspective

Consider a scenario where a user parks their vehicle in the parking lot of a restaurant and connects the vehicle to the charging station. The user provides setting preferences, such as selecting whether to charge or discharge the battery possibly by entering a bid, the minimum threshold for the battery level the user would like to have in the vehicle, the minimum distance in miles that the user needs to travel, and the duration of time the user expects to be at the restaurant.

New requirements, such as the need to leave the restaurant sooner or to visit other destinations, result in changes to the user options. The change in charging requirements will result in a new charging schedule for the vehicle. This schedule is implemented by the charging station energy management logic, which involves a number of constraints and options, such as maximum charging speed, loading of the circuits and the utility transformer, and constraints associated with utility operations, such as local voltage levels. *Assuming that logic exists to determine the new energy charging schedule, the question that we need to address is how can the system ensure that the necessary exchanges of information among the user, the vehicle, the charging station, the payment management company, and the utility take place in a secure manner.*

Vehicle Perspective

There can be physical as well as cyber security issues related to the vehicles. Alerts should be triggered for any integrity violations. *How is the physical integrity of the vehicle preserved (i.e., the vehicle is not damaged) using a secure cyber layer?* Also, communications among legitimate vehicles must be secured.

Vehicle Battery Perspective

Access control to install and uninstall each vehicle's battery may affect the security system (cyber security) of the vehicle knowing that the adversary can perform cyber attacks. *How to control (grant or revoke) and securely verify legitimate access by individuals involved in the vehicle's battery installation or replacement? And by extension, how to verify that these individuals deployed the appropriate configuration settings while installing or replacing a vehicle's battery?* Precise care should be taken in such a scenario using remote attestation with the server. A common requirement for the remote attestation is that a distinct security service that allows a trusted party to check the internal state of a remote embedded device, such

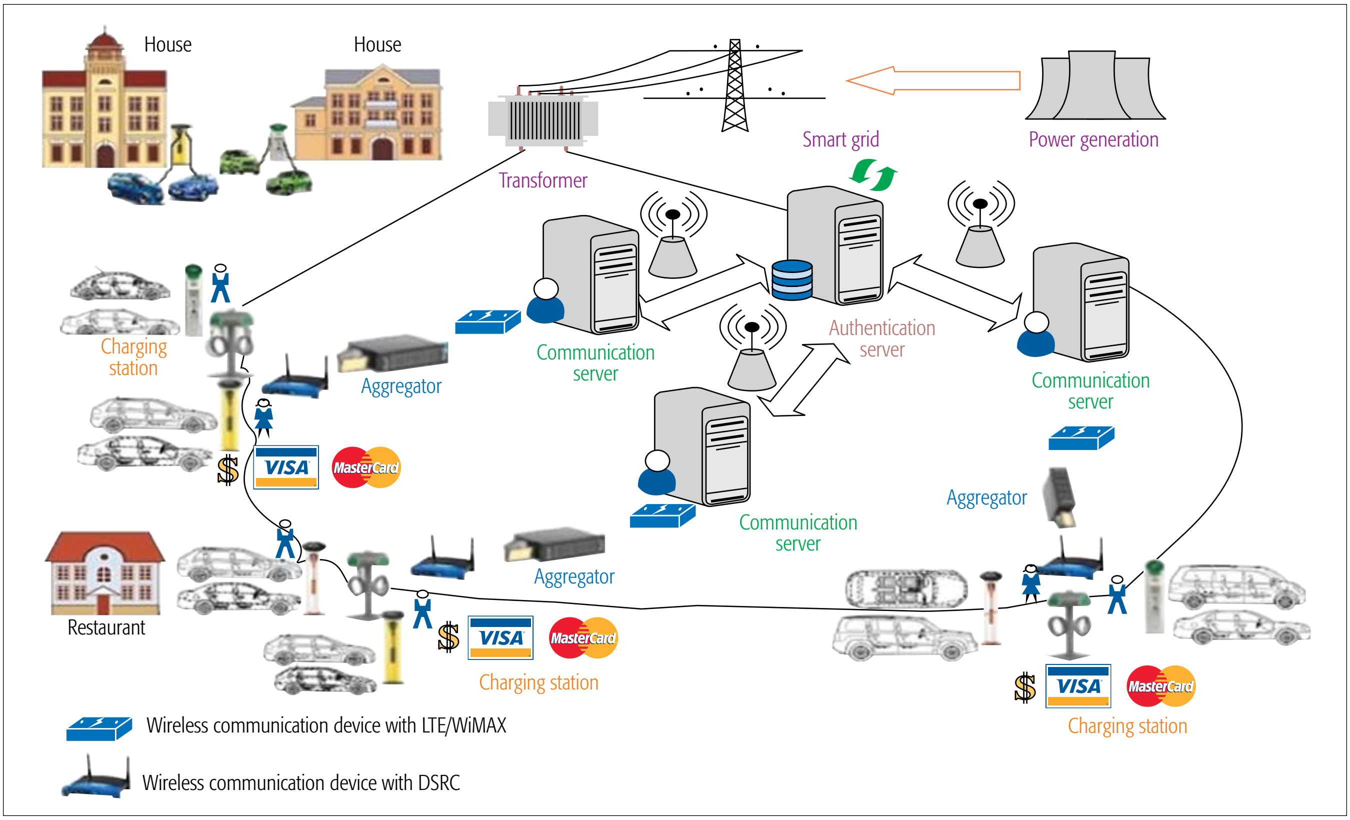

Figure 1. A scenario of smart charging and discharging in the V2G network.

as a vehicle's battery, should be allowed. Supply chain cyber security should also be provided to the vehicle's battery in order to minimize the risk of information theft, intentional damage, and malware activities.

Electric Utility Perspective

The main objective of the power company is to deliver reliable electricity to customers (through EV charging stations), and also to transfer power back from the vehicle to the grid during the discharging operation. In order to accomplish this, the power company must ensure that various electrical quantities (such as voltages and power flows) in the circuits are maintained within operational limits. For instance, simultaneous charging of various vehicles in a circuit may create an electric overload in the transformer, or an under voltage condition. These conditions are both dangerous and costly. The charging of various electric vehicles must therefore be coordinated and scheduled dynamically. This requires the real-time exchange of information between the vehicles, the charging stations, and the utility. Hence, network security and privacy are of paramount relevance since it may affect the physical behavior of the electric vehicles and other devices connected to the smart power delivery network.

Billing Company Perspective

A real-time pricing system needs to be implemented for billing purpose immediately following the charging or discharging operations. For the consumed power units, a final bill can be generated on a weekly/monthly basis and/or based on prepaid and post-paid user categories, whereas the user is expected to be paid immediately after finishing each discharging operation. In the current scenario of the V2G system, the real-time state of charge (SoC) information of each battery is communicated to the controller or aggregator in order to figure out the pricing for real-time charging or discharging power units [5]. However, this violates the privacy of vehicles, as the aggregator may then be the source of the vehicles' information leakage and modification.

Privacy and Security Challenges

This section describes in more detail various privacy and security challenges of V2G networks, which include: linkability with previous sessions, the possibility of security attacks, identity tracing, deriving location information, extracting vehicle preferences, and compromising message information.

Information Privacy: Information privacy is referred to as the permissible use of information. Consumers have the right to privacy regarding energy consumption. To protect consumers' privacy, power utilities or third parties are responsible for implementing right to access policies that ensure consumers' information is accessed and used only for legitimate utility-related purposes. Consumers' information, such as their identity, vehicle daily power usage and location, should not be made available to third-party service providers without the full knowledge and consent of the consumers. When utilities and third parties use information that is provided or entrusted to them, the information should be used according to the agreed purposes that protect the privacy of the consumers. Therefore, it must be required that third parties have in place appropriate security mechanisms in accordance with the NIST Smart Grid Cyber Security Strategy and Requirements

(NISTR 7628) [6] that allow access to information only within the context of authorized users' official capacity. Consumer data contains important pieces of information including specific times/locations of electricity use, type of operation requested (charging or discharging) and/or vehicles used. Analysis of this data can reveal consumer behavior, hence power utilities and third parties have a responsibility to ensure the appropriate level of protection over consumer information.

Consumer data contains important pieces of information including specific times/locations of electricity use, type of operation requested (charging or discharging) and/or vehicles used. Analysis of this data can reveal consumer behavior, hence power utilities and third parties have a responsibility to ensure the appropriate level of protection over consumer information.

Information Security: Information security is commonly represented in terms of the confidentiality, integrity, and availability of information. Information security comprises practices and processes, such as encrypting the transmitted information between the charging station and the aggregator, thus ensuring that the information is protected against any unauthorized access. Employing security mechanisms, such as hash or message authentication code at the aggregator, communication server, control center, and billing center, ensure that the message content is unaltered (i.e., information integrity is preserved) and the message is accurately received when sent over the network. It is also imperative that when needed, the information is available and accessible by the legitimate parties.

The security and privacy requirements of V2G networks extend the basic requirements of vehicular networks and financial transaction networks. The V2G network has a higher level of scale and complexity due to the fusion and integration of technologies from several domains as well as in the diversity and large volume of stakeholders involved across industries. Some of these industries are transportation and its safety, information communication technology (ICT), investor-owned utilities and municipal power entities, EV and EVSE manufacturers, the energy commission, and third-party aggregator providers. As a result, the security and privacy challenges increase significantly for V2G networks as compared to traditional communication networks. The uniqueness of the V2G network requires charging and discharging of the mobile vehicle's battery across centralized and distributed networks, a secure payment system with debit as well as credit functionalities for the vehicle owner at large because of frequent charge and discharge of the battery, remote attestation: control and verification of legitimate access to allow battery installation and uninstallation securely, and performing different operations (addition/multiplication) over the encrypted data, such as computing aggregated power demand needed for a certain area. There is no such need for performing operations over encrypted data in traditional smart phone payment systems. The V2G system deals with such operations in order to monitor total supply and demand of power in each geographic area.

Next, we enumerate traditional security and privacy challenges as well as unique challenges for V2G networks.

Privacy Challenges

The privacy challenges in the V2G network are the following.

How to Keep a Vehicle's Identity and its Location Information Untraceable from the Aggregator? The identity of the vehicle may be compromised [5, 7], as the aggregator retrieves the vehicle's information and can misuse it by passing the information to an adversary. The aggregator or operator can also keep track of vehicle-specific information, such as the location of the charging station and how long a vehicle was at that charging station. The timing patterns of the owner of the vehicle can also be traced, if the vehicle frequently charges or discharges at a specific charging station.

How to Protect the Privacy of the Vehicle's Other Preferences? Revealing the vehicle owner's selection of performing charge or discharge operation and SoC of each vehicle's battery (current battery status and percentage of battery the vehicle owner wishes to charge or discharge) leak private information to the collector or aggregator [5, 8].

An adversary can retrieve this information and store user history. User history can reveal information about when the vehicle owner frequently moves from one location to another on a daily basis, where do they go on the weekends, how far they travel in a day, which parking lot they use most often, and which bank they frequent most often.

What Information is Required for Billing? The control center or the bill center requires the user and vehicle identity and SoC related information of the vehicle's battery, such as the identity code of the battery, whether the charge or discharge operation is selected, battery SoC to check whether the battery is fully charged (and thus cannot charge anymore), fully discharged (and thus cannot discharge anymore), or in a charging or discharging state, how much battery level was charged or discharged and in what duration, and the amount of power units consumed during charging or discharging for billing purposes. This charge or discharge data can reveal private information about the vehicle's battery and its owner.

Security Challenges

Security challenges in the V2G network are discussed below:

What if a vehicle misbehaves? A vehicle may misbehave in a certain way, such as providing wrong information to the aggregator. The operator needs to first verify whether a vehicle has conducted a wrong attempt or it has been compromised by the adversary, and then run a process of repudiating the vehicle from accessing the V2G network.

Is There a Linkability Issue? It may be possible that the adversary can obtain the user's daily routine information by linking previous connections with the current one. It may also happen that in a current session the same information is resent as it was sent in a previous session. An unlinkable process is required where the outcome of each session must be different so that the adversary cannot correlate captured information between sessions.

What if an Adversary Performs Attacks? An adversary may perform attacks over the V2G network, such as MITM attacks, replay attacks, redirection attacks, impersonation attacks, repudiation attacks, and flood-based DoS attacks. The proposed solution for the V2G network must be able to defeat such attacks. The following scenarios describe different attacks over the V2G network.

Unlike the smart phone payment system where only payment information is compromised in the event of any attack, the V2G system not only deals with information modification over the communication network but also its effect on the power system. Hence, the V2G system regularly runs power algorithms, such as power flow, state estimation, and contingency analysis.

Impersonation Attack: If the adversary knows the identity and/or session key of the victim vehicle or the aggregator, it can perform an impersonation attack. There are two possible cases of this attack:

- *Case-1: The Adversary Impersonates the Vehicle:* The adversary uses a fabricated identity, generates a hash of the message, and sends the complete message to the respective aggregator on behalf of the victim vehicle.
- *Case-2: The Adversary Impersonates the Aggregator:* A malicious aggregator sends fabricated information to the vehicle on behalf of a legitimate aggregator. The information may include the victim aggregator's identity and a fake response to the vehicle's request.

MITM Attack: The adversary may build an active connection between the vehicle and the aggregator or the communication/authentication server as enumerated in the following cases:

- *Case-1: Key-Exchange by the Adversary:* The adversary can establish a connection with the vehicle and the aggregator or the server. The adversary can generate a shared secret key if the vehicle/server's private key is compromised or if the source entity's identity and signatures are not verified.
- *Case-2: The Adversary as a Rogue Aggregator:* The adversary may install a fake aggregator, extract information provided by the vehicle and later use this information to access the system from a legitimate aggregator.
- *Case-3: The Adversary as an Insider Attacker:* A friend who has access to the vehicle, and knows the security keys, can perform malicious activities without the owner of the vehicle knowing.
- *Case-4: The Adversary Tries to Extract Secret Information:* The adversary can try to extract information from the messages transmitted between the vehicle and the aggregator during protocol run.

Replay and Injection Attack: The adversary can intercept, inject, or re-send previously sent messages in order to perform a replay attack.

Redirection Attack: The adversary can advertise itself as a legitimate aggregator over the network, and as a result, legitimate vehicles connect to the malicious aggregator and are then compromised.

Known Key Attack: The adversary can correlate previously generated known keys in an attempt to extract some useful information.

Repudiation Attack: The owner of the vehicle or their friend may deny performing specific actions, operations, or transactions, thus resulting in a repudiation attack.

Flood-Based DoS Attack: The adversary can perform a DoS attack by sending a disproportionately large number of charging or discharging requests to the aggregator, establishing half-open connections and refusing to complete the connections, thus eventually exhausting the network resources of the aggregator. This would create a denial of service for legitimate vehicles in need of power services.

Unique V2G Challenges and Characteristics

A V2G system is a cyber-physical system (CPS) consisting of interacting elements with physical input and output instead of stand-alone devices, while the traditional system such as a mobile payment system is not a CPS. Unlike the smart phone payment system where only payment information is compromised in the event of any attack, the V2G system not only deals with information modification over the communication network but also its effect on the power system. Hence, the V2G system regularly runs power algorithms, such as power flow, state estimation, and contingency analysis.

We also discuss the unique challenges and characteristics of the V2G networks.

Dynamic Participation: Electric vehicles can dynamically join and leave networks without influencing ongoing communications. The vehicles may connect to the charging station individually or in a group. This dynamic participation of the vehicles presents novel challenges with coordinating charging schedules across the network in order to smooth out energy demand.

Vehicle Mobility: The vehicles may connect to the charging station in the home or visiting area networks. The home area network refers to the geographic area where the vehicle resides and is registered, whereas the visiting area network includes locations outside the home area of the vehicle. Generally, the smart phone payment systems, such as Alipay, a third-party online payment platform, do not protect the sender's identity, that is, they do not provide anonymity. A payment system in the V2G system supports the charging and discharging payment transactions, providing user anonymity during the entire transaction even when an EV transacts in a visiting area.

Centralized and Distributed Networks: The existing power grid is operated as a centralized entity, whereas the smart grid is designed to work in a distributed manner. However, the smart grid needs to work in both modes until the migration is completed. An example of operating in both modes is when the vehicle's charging and discharging is performed in the distributed network, whereas only the vehicle's discharging is allowed in the centralized network [1, 9]. The V2G system requires the distributed and centralized networks to charge and discharge the battery of the vehicle at a charging station along with a secure payment system to support these operations.

Role-based Vehicles and Payment System: The electric vehicle acts as energy consumer, energy storage, and energy supplier while performing charge, idle, and discharge operations, respectively. Further, the state of the vehicle's battery can be charging, fully-charged, and discharging. The traditional approaches that only consider the vehicle as energy consumer are not directly applicable in V2G networks.

The V2G payment system is different from the smart phone payment system because unlike the unidirectional (one-way) smart phone payment system wherein the consumer always pays the vendor, the V2G payment system is a bi-directional (two-way) payment system for charging and discharging payment transactions with the owner of the EV being able to either buy power from the grid as an energy consumer or sell power to the grid as an energy provider.

Proposed Architecture for a Secure Smart V2G Network

In this section, first we discuss the security and privacy objectives that are required to be achieved, and then describe our proposed architecture for the V2G network.

Security Objectives

The proposed solution must satisfy the following security objectives in the V2G network:

Mutual Authentication: The V2G network must provide mutual authentication between the vehicles and the aggregator and/or the registration authority. This process helps protect the network against redirection and impersonation attacks. The vehicles at a charging station must be able to communicate with the aggregator securely, and no unauthentic or malicious vehicle should be able to connect for charging or discharging operations.

Information Confidentiality: This is one of the mandatory objectives of the V2G network. Private information must be secret or hidden in order to provide confidentiality to the transmitted information. Encryption is used to provide confidentiality to the messages.

Message Integrity: The integrity of all transmitted messages in the V2G network must be maintained. For each sent message, it is required to verify whether any violation has taken place during message transmission.

Privacy Objectives

The privacy of the EVs must be preserved whenever EVs access charging stations. Also, the privacy of the consumers must be maintained when the utilities share consumer data with third-parties. The proposed solution must satisfy the following privacy objectives in the V2G network:

Identity Anonymity: The identity of the vehicle should not be disclosed, as an untrusted aggregator can also receive the vehicle's information and can misuse the information by passing it to an adversary.

Vehicle Untraceability: The scheme should maintain vehicle untraceability so the adversary cannot distinguish whether two different messages (with pseudo-identity and/or vehicle's location, battery status, and selection of charging/discharging with timing information) originated from the same or two different vehicles. The scheme satisfies untraceability if the adversary cannot guess the correct message-vehicle pair with a probability higher than random guessing.

Forward Privacy: Forward privacy is similar to untraceability but with additional capabilities. Two identical messages are generated. One of the two messages is passed on to the adversary. Forward privacy is maintained if the adversary, without having either a secret or session key, is still unable to trace previous sessions.

Proposed Architecture

We propose a new architecture for secure smart charging and discharging of vehicles as shown in Fig. 2 that involves m-charging stations, at most n-electric vehicles (and/or hybrid vehicles) charging or discharging at a charging station, k-aggregators geographically distributed, r-communication servers at different locations, and one or more authentication servers in the network. The uniqueness of the proposed architecture involves the dynamic verification support for charging and discharging of the vehicle battery by anonymous signatures, a secure payment system support for frequent financial transactions by the vehicles by using an anonymous payment system, remote attestation support for control and verification of legitimate access to allow battery installation and uninstallation securely by using anonymous authentication and fine-grain access control, and other supporting modules for performing different operations (addition/multiplication) over the encrypted data, such as computing the aggregated power demand needed for a certain area by using homomorphic encryption. Our proposed system architecture includes a scheme with various security and privacy features, such as:

1) Anonymous authentication and fine-grained access control
2) Anonymous signatures
3) Information confidentiality and message integrity
4) Remote attestation
5) Payment system in the V2G network.

We summarize the V2G security and privacy requirements with these features of our scheme in Table 1 in order to achieve the desired goals.

Functional Description of the Proposed V2G Network Architecture: Figure 2 presents the overview of the proposed architecture, where the scheme executes in five different steps ((1) to (5), yellow arrow). Figure 2 shows the communication between an aggregator (LAG) and a communication server (ComS). Similarly, the scenario can be extended with several aggregators and communication servers. Vehicle owners connect their vehicles (EV_{11}, EV_{12}, ..., EV_{mn}) to charging stations for charging or discharging their batteries. The owner provides its input preferences (SoC) and then waits for the system to process the inputs. The aggregator, deployed over the wireless network (i.e., DSRC), concentrates vehicle information and forwards that information to the communication server over the wide area network, i.e., long term evolution (LTE). The communication servers are responsible for securely receiving the vehicles' information, communicating with the authentication server, control center, and billing generation and payment management center, and finally forwarding the control center's decision of granting/revoking the requested operation based on the demand-supply requirements of the vehicles. The communication server transmits the vehicles' received information, such as pseudo-identities and secret parameters, to the authentication server. The authentication server verifies whether the participating vehicle belongs to a legitimate set of vehicles in the network, and sends a response back to the communication server. This process can be executed in a batch, given that many communication servers can request the vehicle verification simultaneously. Thereafter, the communication server interacts with the control center and performs demand-supply analysis for the specific application. If the control center allows the requested operation (charging/discharging), the communication server notifies the vehicle and then transmits some of the vehicle's information

Forward privacy is similar to untraceability but with additional capabilities. Two identical messages are generated. One of the two messages is passed on to the adversary. Forward privacy is maintained if the adversary, without having either a secret or session key, is still unable to trace previous sessions.

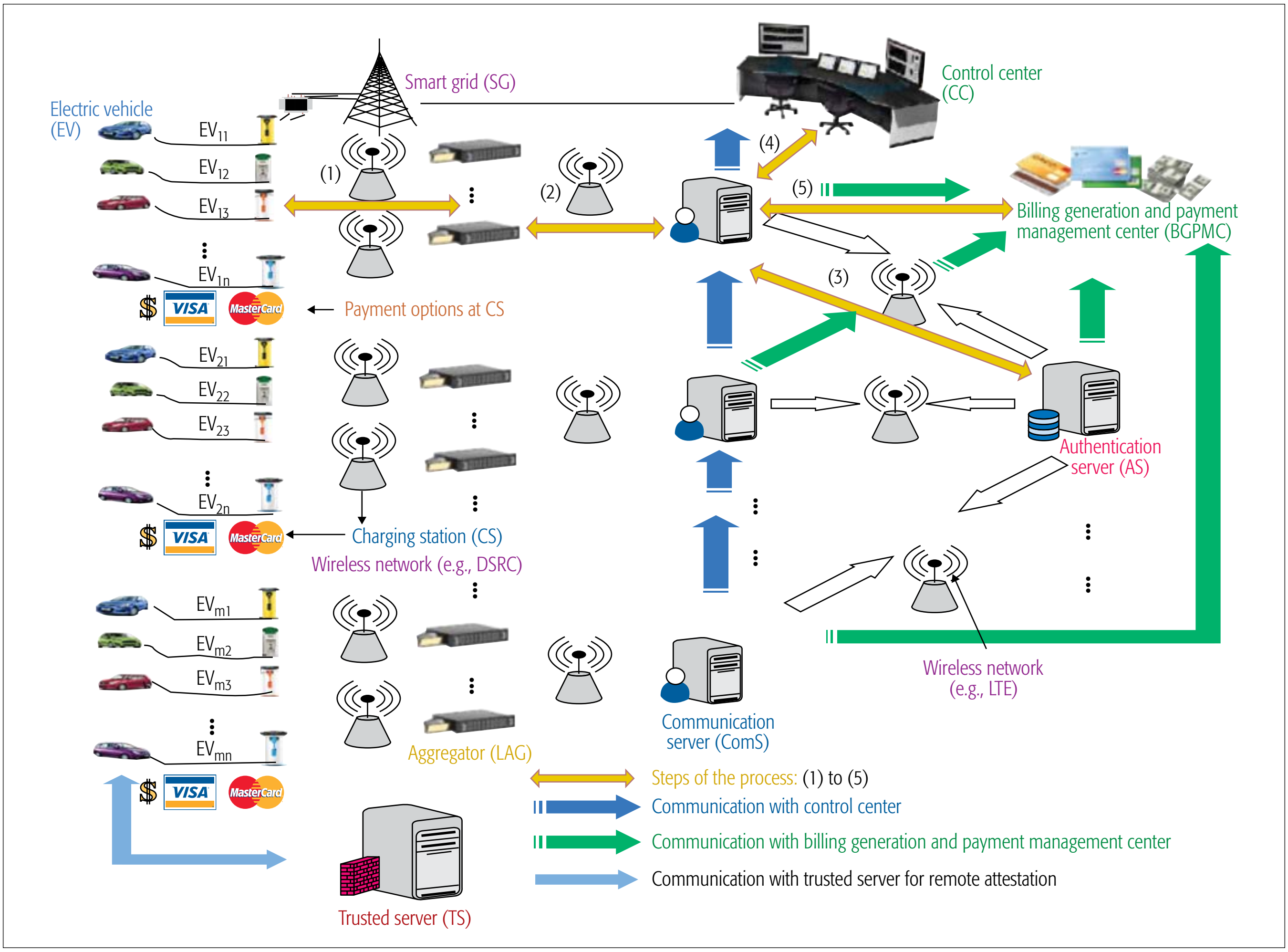
Electric vehicle (EV)
EV_{11}
EV_{12}
EV_{13}
EV_{1n}
EV_{21}
EV_{22}
EV_{23}
EV_{2n}
EV_{m1}
EV_{m2}
EV_{m3}
EV_{mn}
VISA
MasterCard
Payment options at CS
Smart grid (SG)
Control center (CC)
(1)
(2)
(3)
(4)
(5)
Billing generation and payment management center (BGPMC)
Authentication server (AS)
Charging station (CS)
Wireless network (e.g., DSRC)
Aggregator (LAG)
Communication server (ComS)
Wireless network (e.g., LTE)
Trusted server (TS)
Steps of the process: (1) to (5)
Communication with control center
Communication with billing generation and payment management center
Communication with trusted server for remote attestation

Figure 2. Proposed architecture of smart charging and discharging in the V2G network.

to the billing center. The billing center verifies the vehicle information and performs the debit or credit transaction depending on the service requested operation. Finally, the process loop is closed when the vehicle undertakes and completes the approved charging or discharging operation.

The different parts of the proposed V2G network architecture interact in the following way:

Step 1: First, the vehicle connects itself to the charging station for charging or discharging the battery. The proposed architecture provides identity anonymity and vehicle untraceability by running the "Anonymous Authentication and Fine-Grained Access Control" module with appropriate access control policy.

Step 2: Anonymous data transfer takes place between the vehicle and the aggregator. The aggregator establishes a connection to transmit private and confidential information of the vehicle securely using techniques such as additively homomorphic encryption. The aggregator forwards the received vehicle's information to the communication server in a secure manner. The communication server sends a part of the information to the authentication server for vehicle identity or pseudo-identity verification through a dynamic accumulator, and also transmits other parts, such as the aggregated power demand to the control center.

Step 3: The authentication server verifies the vehicle's identity and other secret information by techniques such as dynamic accumulator in a batch, and sends its response back to the communication server. The authentication server also verifies trust security services, such as the state of the battery of each vehicle, using the "Remote Attestation" module.

Step 4: The control center uses the received information (in step 2) to analyze demand-supply of the power at regular intervals, and announces its decision to accept/reject the charging/discharging vehicle's request to the communication server. The communication server notifies the vehicle about the control center's decision. During the entire process, confidentiality and integrity of the information must be maintained by the "Information Confidentiality and Message Integrity" module. If the vehicle needs to edit its preferences or needs to reconnect to the charging station within a session, the vehicle has to provide its anonymous signature with other details using the "Anonymous Signature Scheme" to the aggregator, which then forwards the information to the communication server for further processing.

Step 5: After the completion of the vehicle's charging or discharging operation, the process flow is directed toward the Billing Generation and Payment Management Center (BGPMC), which uses the "Payment System" module to credit or debit the transaction amount depending on the operation performed by the vehicle.

Note that anonymous authentication is different from anonymous signature. Anonymous authentication is a means of authorizing a user without identification. Anonymous authentication helps the recipient verify that the sender is a legitimate user of the system. An anonymous group/ring signature scheme proves that the messages received by the recipient were sent by a legitimate sender. In the proposed scheme, anonymous authentication proves that the sender belongs to a set of legitimate users. If the sender verification is successful, the user is authenticated for a session based on the expiration time of the session. On the other hand, the sender uses an anonymous signature scheme using its own privacy key and the public keys of other users while sending a message to the recipient, and the recipient verifies that the signature was generated by a legitimate user. The authentication process ensures that the user is legitimate to the system while the signature ensures that the message was generated and sent by a legitimate user.

Information confidentiality helps prevent MITM attacks. The use of random numbers or timestamp values with transmitted messages prevents replay attacks. Verifying the correct location of the vehicle by the communication server stops redirection attacks. Mutual authentication provides protection against impersonation attacks. The use of digital signatures defeats repudiation attacks. Verifying half-open connection requests of the malicious vehicles by the server prevents flood-based DoS attacks. If the server does not receive a response from the vehicle, the half-open connection is terminated by the server.

The following subsections provide a detailed description of the security and privacy related features of the proposed architecture.

Anonymous Authentication and Fine-Grained Access Control: The V2G network requirements are different from typical authentication systems. It requires anonymous authentication of the vehicles so that the aggregator cannot learn the vehicles' personal information. In other words, the scheme must maintain identity anonymity and untraceability properties. Only the authentication server knows and verifies the actual identity of the vehicle, but the intermediate entities, such as communication servers and aggregators, do not.

An option for vehicle verification could be the use of a trusted third party that provides resource access to the authentic users. However, the third party can be compromised externally or by malicious insider operators. The third party can be replaced by a secure multi-party (vehicle) computation (SMPC) technique using verifiable secret sharing that involves multiple vehicles computing an agreed function (such as addition, multiplication, and comparison of the secret shared values without knowing the actual secrets) with inputs from each vehicle in such a way that none of the vehicles can know the input of any other vehicle, and the only information each vehicle acquires from the SMPC computation is the public output. Hence, no vehicle gets the complete secret, but only a part of it. A complete secret can only be reconstructed by the aggregator, if it receives more than a threshold number, say *t*, of the shared values. The SoC information (and also other information, such as traffic and accident related information) can be sent by each vehicle to all other vehicles it chooses to connect to. The aggregator then collects all the information by grouping each SoC attribute, and uses this information to calculate the aggregated energy demand over the confidential data.

Requirements	1	2	3	4	5
Vehicle owner perspective requirements					
Input information for charging or discharging	✓				
Input user profile preferences	✓	✓			
• Minimum level of the battery needed	✓	✓			
• Distance to the destination place (miles to go)		✓			
• Expected time to stay		✓			
Input sudden changes in the user preferences	✓	✓			
• Urgent move (waiting time is suddenly down to zero or a few minutes)	✓	✓			
• New distance to be covered	✓	✓			
Vehicle perspective requirements					
Secure communication by the vehicles involve in charging and discharging of the power			✓		
Connection of the vehicle to the legitimate aggregator or server	✓				
Detection of integrity violations			✓		
Battery perspective requirements					
Control and verification of legitimate access to allow battery installation and uninstallation securely	✓			✓	
Utility or power company perspective requirements					
Estimation of total power demand requirement over the encrypted data (at control center)		✓	✓		
Anonymous decision of grant or revoke charging and discharging of the vehicles (by control center)		✓	✓		
Secure communication between the charging station nodes and the utility			✓		
Bill generation center perspective requirements					
Secure transmission of the SoC information for billing purpose	✓	✓			✓
Secure and privacy-preserved payment system for charging and discharging of the vehicles					✓

TABLE 1. V2G security and privacy requirements with the features of our scheme.

In fact, anonymous authentication can be achieved using various techniques, such as ring signature, blind scheme, and partially blind scheme. Electric vehicles in V2G networks are dynamic in nature, as many vehicles leave and join the network frequently. Therefore, forming a dynamic group at each distinct geographic area (for a single or a set of charging stations) can handle such situations. Once a dynamic group is formed, an initial key agreement is processed that allows vehicles to join and leave the network. However, it is required to ensure that a change in the group structure will accurately change the corresponding group key in order to preserve key independence without affecting other vehicles' participation.

Anonymity ensures that the aggregator cannot know the identity of the vehicle, but rather only verifies that the vehicle belongs to an authorized group of vehicles. This requirement can be achieved by using a dynamic accumulator with addition, evaluation, and deletion of the vehicle. The proposed scheme for V2G networks should not be deniable. A scheme is deniable if the aggregator or server cannot verify that other parties (such as EVs) participated in the system. Non-deniability can be achieved in the network via zero knowledge proof, wherein an EV proves a true statement to the aggregator or server.

Additionally, a fine-grained access control policy is applied to manage large queues of public vehicles, priority service vehicles, and private vehicles [10]. The utility can also reserve some charging stations devoted only to priority-service vehicles.

Anonymous Signature Scheme: In order to protect vehicle identity while signing a message, blind signatures allow the aggregator to easily verify that the signature belongs to one of the vehicles among a set of registered vehicles. However, the aggregator cannot identify the actual vehicle that had signed the message. The following are some strategies to achieve anonymous signatures.

Ring Signature and Group Signature: Ring signatures can be used in situations where a queue is maintained by a charging station for providing services to a large number of vehicles. A small number of groups with limited vehicles can be formed from a large queue for efficient processing. A vehicle can create a ring signature using the ordered public keys of all member vehicles of the group. One of the differences between ring signatures and group signatures is that ring signatures are efficient (no group manager, no setup and revocation procedure, and no co-ordination), and do not require any trusted authority. Ring signatures also provide anonymity, whereas the anonymity of a signer can be revoked in group signatures, that is, the signer can be traced by a group manager. While generating a ring signatures in a V2G network, any vehicle can choose any number of possible signer vehicles (including itself) and sign a message using its secret key and other vehicles' public keys, even without receiving other vehicles' approval.

For an ideal group signature scheme that supports a large group of vehicles, the length of the group public key, group private key, and signatures should be independent of the number of vehicles in the group. In addition, the scheme should also enable adding new vehicles in the group without updating the group public key, and be able to handle group member revocation. Revocation efficiency can be improved by adopting a dynamic accumulator.

Blind Signature: Blind signatures are used in situations where a signer (vehicle) is required to sign a message without viewing its content. This blindness property is applicable in various applications, such as electronic voting, untraceable electronic cash, anonymous fingerprinting, unlinkable credentials, and so on. However, these signatures have shortcomings since the signer has no control over the message parameters. Some random values are embedded in the message, and thereafter the signer sends the message. After receiving the signed message from the signer, the recipient (aggregator or server) filters out the embedded values in order to get a valid signature [11].

Partially Blind Signature: Partially blind signatures resolve some of the existing issues in blind signatures. For example, a blind signature generated by the signer needs to be regenerated after the previous signature expires. Since the signer does not know this information, it has to generate another signature as expected. This increases the overall overhead generated by the signatures. On the other hand, partially blind signatures allow a signer to explicitly declare the information agreed with the receiver. This information could be the creation time of the signature, the expiration time of the signature, and other required conditions. In fact, partially blind signatures are controlled by the signer while the blind signatures are controlled by the receiver.

Threshold Blind Signature: A group of signers blindly participate in a process to generate a threshold blind signature, and the signature can only be verified by the signed values of at least a specified number of signers [12]. In fact, multi-secret sharing is more applicable where different attributes of SoC can be signed and sent to the aggregator.

In summary, a partially blind signature is suitable for V2G networks because a vehicle can create and send its signature with explicit information to the aggregator. More specifically, a restrictive partially blind signature can be used to maintain vehicle privacy, such as a vehicle's identity protection. Furthermore, a threshold blind signature is applicable in a V2G network where a vehicle needs to communicate with the server in the various stages of completing a task, such as reporting malicious behavior or incidents and multi-signatures for secure transactions.

A partially blind signature is suitable for V2G networks because a vehicle can create and send its signature with explicit information to the aggregator. More specifically, a restrictive partially blind signature can be used to maintain vehicle privacy, such as a vehicle's identity protection.

Information Confidentiality and Message Integrity: Information confidentiality and message integrity are strongly required in order to secure transmitted messages over a V2G communication network. Homomorphic encryption can be a good solution for securing aggregated information. It maintains end-to-end information confidentiality by enabling the transmission of encrypted messages from the vehicles to the aggregator. However, the aggregator cannot decrypt the message information, but rather performs different operations over the data received from various vehicles, such as total aggregated battery energy demand. Furthermore, instead of an encryption scheme, another suitable solution is the use of a commitment scheme via perfectly binding or perfectly hiding that involves two phases: commit and reveal. In a V2G network, this commitment scheme allows a vehicle to choose a commit value (secret value) while keeping it hidden to others, but reveals the commit value to the aggregator and/or control center later. Ciphertext-Policy Attribute Based Encryption (CP-ABE) can also be used to enable charging requests of the vehicles without violating the privacy of their SoC attributes. Additionally, a pseudo-identity for the EVs should be used during communications over the network while performing charge or discharge operations.

Maintaining message integrity is also required in a V2G network, as an adversary can alter message information. An adversary can also tamper with messages sent from the vehicles to the aggregator, and as a result the aggregator calculates a wrong aggregated result and consequently performs the wrong supply-demand analysis. In order to provide message integrity, a hash or message authentication function (MAC) is used. Encryption and integrity can be used together as encrypt-then-MAC, MAC-then-encrypt, or encrypt-and-MAC. Encrypt-then-MAC is considered the most secure mode.

Remote Attestation in the V2G System: Remote attestation enables a trusted device and the server to know that the running software provides a secure environment for the required operations to be performed [13]. This remote attestation requirement in a V2G system is different from the traditional mobile payment system. The smart phone payment system deals with the user's subscriber identity module (SIM) without a need for remote attestation of the device, i.e., a smart phone. On the other hand, a V2G system requires remote attestation whenever a battery of the vehicle is installed or uninstalled. It is a distinct security service by which the authentication server can remotely verify the state of the battery of each vehicle.

Integrity measures are used to verify information about the software, hardware, and configuration of the system. The hash values are used in the attestation process to verify the identity of the batteries by the remote server. The server trusts that the attested information is accurate, as it is signed by a trusted platform module (TPM) whose key is certified by the certified authority (CA). However, the user's activities can be traced if one has access to the attestation key. Frequent update patches released for the vehicle may create a problem, as new hash values are required to be made available to the server. Also, if TPM keys are compromised, revocation may be an issue. The feasibility of remote attestation without trusted hardware should also be investigated. *We should have such a scheme that resolves the user privacy concerns without the involvement of a trusted third party.*

Payment Systems in a V2G Network: The V2G payment system should be very efficient and secure, and able to authenticate involved parties many times in a day to support smart charging and discharging. On the other hand, the traditional smart phone payment system need not be run so frequently. Smart charging allows a vehicle owner to charge and discharge its vehicle's battery based on inputs, such as how long he wants to charge, what battery level he wishes to keep for the next day, after what battery level he wants to earn profit by discharging battery, and so on. This process frequently repeats, and bi-directional payment transactions take place depending on the charging operation. Also, the smart phone payment system does not provide privacy to the user identity over the network. The V2G system must require a privacy-preserved approach to hide critical information over the network. There are various forms of payment systems today, but many of them are not suitable for a V2G network [3]. These payment systems are paper cash, e-cash, paypal, micro-payment, prepaid cash, and credit or debit card.

Paper cash provides anonymity, but it is not suitable for a V2G system due to the difficulties in managing large payments and security of the system. E-cash also provides anonymity by generating a transaction ID. Normally, e-cash is used for small-amount transactions, and also has a daily limit on the transaction amount. For a V2G system, which requires frequent payment transactions even in a single day, e-cash is not suitable. Paypal is a very commonly used third-party e-payment system. However, if the third party (Paypal) is not trustworthy enough, it may result in user privacy issues, such as location and time of a vehicle performing charging or discharging operation. Furthermore, micro-payments are only suitable for small-amount transactions, and thus is not good enough to consider for V2G systems. Prepaid cash cards are the same as e-cash because you cannot receive payment for a lost card. Although prepaid cash cards provide anonymity, they are not suitable for a V2G system as they support only one-way transactions (charging/debiting the consumer) for the vehicle. Credit or debit cards support two-way transactions, but do not provide user anonymity. The details of the card may also reveal user-related information.

In conclusion, either the card payment solution must provide anonymity for large amounts of frequent transactions, or there should be a new payment system that preserves user privacy and can also provide the required functionality. Recently, a new payment system, designed in [3], proposes a cryptographic solution with an in-car unit to store the identity and secret of the user. However, if an adversary has access to the user's secret, it can spend the money in the user's account. Therefore, a new dynamic and robust payment scheme is required that can handle frequent transactions as well as large payment amounts during vehicle charging and discharging operations.

The V2G system must require a privacy-preserved approach to hide critical information over the network. There are various forms of payment systems today, but many of them are not suitable for a V2G network. These payment systems are paper cash, e-cash, paypal, micro-payment, prepaid cash, and credit or debit card.

Specific Security Mechanisms for the V2G

In this section, we briefly discuss specific security mechanisms for electric vehicles in the V2G networks.

Vidya *et al.* [14] proposed a PKI model that incorporates intra-domain and inter-domain certification management techniques using ECC implicit certifications in the V2G network, as regional transmission companies are tied together with power distribution and generation companies. Liu *et al.* [9] proposed a role-dependent scheme using hybrid cryptographic primitives (e.g., ring signature, fair blind signature, and proxy re-encryption) in which a battery vehicle interacts with the power grid in different roles, that is, energy demand (i.e., as a consumer), energy storage, and energy supply (i.e., as a generator). Saxena *et al.* [1] proposed a scheme using a dynamic accumulator based on a bilinear pairing that handles dynamic connect and disconnect for a number of vehicles from a charging station, and performs secure vehicle operations in the centralized and distributed V2G networks under home area and visited area scenarios.

Conclusion and Open Challenges

This article presented the security and privacy challenges and requirements for smart V2G networks. An architecture has been proposed that provides anonymous authentication and fine-grained access control, information confidentiality and message integrity, remote attestation to grant or revoke common access, verification of battery installation and uninstallation procedure, and a secure payment system for handling large amounts of frequent transactions with anonymity. We discussed a scheme in which by providing anonymous authentication, the original identity of the vehicle can be hidden. Also, partially blind signatures and threshold blind signatures are used to provide vehicles' information to the aggregator without revealing the original identity of the vehicles. Fine-grained access control and remote attestation allow operational access specific to each vehicle and verification of legitimate access to allow battery installation and uninstallation of the vehicle securely. Furthermore, information confidentiality provides secure communications between each vehicle and the aggregator, whereas message integrity checks mandate that each message transmitted over the network is received unaltered. Also, new solutions are required to perform different operations over the confidential data. Finally, an anonymity-based payment scheme is required for handling secure financial transactions related to the vehicles' charging and discharging operations. The proposed architecture and the scheme provide clear guidelines for transmitting confidential information with integrity to intermediate devices or operators while anonymously providing authentication, untraceability, and forward privacy. All of the aforementioned recommendations provide a framework for building a more secure and privacy-preserving smart V2G network, thus making all participants in the V2G network more impervious against security attacks.

The proposed architecture and the scheme provide clear guidelines for transmitting confidential information with integrity to intermediate devices or operators while anonymously providing authentication, untraceability, and forward privacy.

Open challenges in the security and privacy of the V2G network include mobility and dynamic participation of the vehicles, role-based authentication and authorization, and accessibility in the centralized and distributed V2G networks in the home area and visiting area. The crucial challenges for the future V2G network include analyzing cyber-security and cyber-physical security aspects of the V2G system. New methods need to be developed for the identification of cyber-security attacks, their detection, and prevention. Similarly, a cyber-physical V2G system needs to be explored under different attack scenarios, such as bad data injection, malicious command injection, and communication delay in the network, and practical solutions that address V2G system vulnerabilities and misbehavior need to be developed.

References

[1] 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, 2016, pp. 1438–52.

[2] Dedicated Short Range Communications, Intelligent Transportation Systems Joint Program Office, United States Department of Transportation (last accessed on June 7, 2016); http://www.its.dot.gov/DSRC/dsrc_faq.htm.

[3] M. H. Au *et al.*, "A New Payment System for Enhancing Location Privacy of Electric Vehicles," *IEEE Trans. Vehic. Technol.*, vol. 63, no. 1, Jan. 2014, pp. 3–18.

[4] R. Schmidt *et al.*, "V2G Interface Specifications between the Electric Vehicle, the Local Smart Meter, and its Service Providers," *Proc. 7th Framework Programme, INFSO-ICT 285285*, 2012 (last accessed on June 1, 2016); http://www.power-up.org/wp-content/uploads/2012/07/PowerUp_D4.1_final.pdf.

[5] D. P. Ghosh, R. J. Thomas, and S. B. Wicker, "A Privacy-Aware Design for the Vehicle-to-Grid Framework," *Proc. 46th Hawaii Int'l. Conf. System Sciences*, Wailea, USA, 2013, pp. 2283–91.

[6] W. M. Gausman, "NBP RFI: Data Access," (Response to the U.S Department of Energy), Pepco Holdings, Inc., July 2010 (last accessed on June 6, 2016); http://energy.gov/sites/prod/files/gcprod/documents/Pepco_Comments_\\DataAccess.pdf.

[7] Y. Zhenyu *et al.*, "P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2011, pp. 697–706.

[8] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid (V2G) implementation," *Energy Policy*, vol. 37, 2009, pp. 4379–90.

[9] H. Liu *et al.*, "Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, Feb. 2014, pp. 208–20.

[10] V. Goyal *et al.*, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. ACM CCS*, New York, USA, 2006, pp. 89–98.

[11] O. Blazy *et al.*, "Short Blind Signatures," *J. Computer Security*, vol. 21, no. 5, 2013, pp. 627–61.

[12] A. Boldyreva, "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme," *Proc. Public key Cryptography (PKC)*, Miami, USA, 2003, pp. 31–46.

[13] V. Haldar, D. Chandra, and M. Franz, "Semantic Remote Attestation: A Virtual Machine Directed Approach to Trusted Computing" *Proc. USENIX Virtual Machine Research and Technology Symposium*, Berkeley, USA, 2004, pp. 1–13.

[14] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Security Mechanism for Multi-Domain Vehicle-to-Grid Infrastructure," *Proc. Global Telecommunications Conference (GLOBECOM)*, Houston, USA, 2011, pp. 1–5.

Biographies

Neetesh Saxena [S'09, M'14] (mr.neetesh.saxena@ieee.org) is a post-doctoral researcher in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Previously he was with the Department of Computer Science, State University of New York (SUNY), South Korea as a post-doc and a visiting scholar at Stony Brook University. He earned his Ph.D. in computer science & engineering from the Indian Institute of Technology, Indore. He is a member of ACM and CSI.

Santiago Grijalva [M'02, SM'07] (sgrijalva@ece.gatech.edu) is the Georgia Power Distinguished Professor of Electrical and Computer Engineering, and director of the Advanced Computational Electricity Systems (ACES) Laboratory at the Georgia Institute of Technology. Prior to joining Georgia Tech in 2009, he spent 10 years in the power industry, developing commercial grade algorithms for real-time power system control, optimization, and visualization. He graduated with his M.Sc. and Ph.D. degrees from the University of Illinois at Urbana-Champaign in 1999 and 2002, respectively.

Victor Chukwuka (vchukwuka3@gatech.edu) is a Ph.D. student in the School of Electrical and Computer Engineering at Georgia Institute of Technology. His areas of research include communication systems, MIMO, cyber-physical systems, and power system dynamics.

Athanasios V. Vasilakos (athanasios.vasilakos@ltu.se) is a professor at the Lulea University of Technology, Sweden. He served as an editor for many journals, such as *IEEE Transactions on Network and Service Management*, *IEEE Transactions on Cloud Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Cybernetics*, *IEEE Transactions on Nanobioscience*, *IEEE Transactions on Information Technology in Biomedicine*, and *IEEE Journal on Selected Areas in Communications*. He is the General Chair of the European Alliances for Innovation.