ACCEPTED FROM OPEN CALL

SECURING VEHICLE-TO-GRID COMMUNICATIONS IN THE SMART GRID

YAN ZHANG AND STEIN GJESSING, SIMULA RESEARCH LABORATORY AND UNIVERSITY OF OSLO
HONG LIU AND HUANSHENG NING, BEIHANG UNIVERSITY
LAURENCE T. YANG, HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY AND ST. FRANCIS XAVIER UNIVERSITY
MOHSEN GUIZANI, QATAR UNIVERSITY

ABSTRACT

Using vehicle-to-grid (V2G) services, battery vehicles (BVs) may help the smart grid alleviate peaks in power consumption. However, wireless communications infrastructure between BVs and the smart grid also introduce severe and unprecedented security vulnerabilities. In this article, we discuss V2G network architectures and present state-of-the-art security, including different security challenges during V2G power and communications interactions. Then we report on our context-aware authentication solution for V2G communications in the smart grid. Finally, we describe several open issues for secure V2G networks.

INTRODUCTION

The smart grid is the next-generation power grid that will transform the traditional power grid into the future "Internet of energy." The conventional centrally controlled electrical grid is facing a variety of new challenges, including aging distribution networks, renewable energy integration, stability, and cyber security. These challenges have motivated a global development to study greenness, security, efficiency, survivability, autonomy, and intelligence in the smart grid. The smart grid is based on a two-way communications infrastructure, which enables customers and electricity providers to cooperatively manage and monitor power usage [1]. A variety of wireless communications technologies will be integrated in the communication architecture to support the smart grid.

In the smart grid, vehicle-to-grid (V2G) is a critical network service, and has received increasing attention [2]. Figure 1 illustrates a V2G network architecture, mainly including three entities: battery vehicles (BVs), local aggregators (LAGs), and a central authority (CA):

- A BV is owned by an individual and connects to a charging station from time to time when its power decreases below a certain level and its battery needs charging.
- A LAG is the power and wireless communication service access point for BVs.
- The CA acts as a trusted entity that belongs to an independent institution; it participates in all communications, and it can derive detailed power and information data to support billing services.

Consequently, in the V2G network, BVs are connected to the power grid for power and information services via LAGs. On the other hand, LAGs directly communicate with the smart power distribution and communication network on behalf of the geographically dispersed BVs. Accordingly, each BV has two simultaneous connections with its current LAG: one power line and one wireless communication link. The LAG is part of the electricity distribution infrastructure of the smart grid. The main functions of the LAG include power charging/discharging management, power status monitoring, and power load scheduling. The LAG also communicates with its current BVs to exchange energy-related information (e.g., time left until fully charged and discharging rate). In terms of the trust relationships in the smart grid, the CA is the only entity trusted by all other entities, and no other straightforward trust relationships exist between BVs and LAGs.

The communications infrastructure between BVs and the smart grid can facilitate better power load management, and hence improve energy efficiency and reliability. However, the infrastructure may suffer from severe security attacks and vulnerabilities [3]. Security and privacy issues are becoming very significant for V2G networks. In the literature, there are only a few studies on privacy and security issues in V2G networks, although several studies have been performed to enhance security and preserve privacy in the smart grid in general. Yang *et al.* [4] identified the emerging privacy issues in V2G networks, and proposed a reward scheme to balance the trade-off between the participants' freedom of using their BVs and the benefits that can be achieved by the power

1536-1284/13/$25.00 © 2013 IEEE

operators. A secure communication architecture was built to achieve privacy-preserving BV monitoring, in which an ID-based blind signature was introduced to enhance anonymity. Guo *et al.* [5] proposed an authentication protocol to deal with multiple responses from a batch of vehicles. The proposed scheme introduced the concept of interval time for an aggregator verifying multiple vehicles, and the aggregator broadcasts a signed confirmation message to inform multiple vehicles using only one signature. The batch verification scheme employs a modified digital signature algorithm. Vaidya *et al.* [6] presented a multi-domain network architecture for V2G networks. The architecture incorporated a hybrid public key infrastructure (PKI) to integrate hierarchical and peer-to-peer cross-certifications. Tseng [7] noticed the privacy concerns created by BV owners' identity information leakage. The work utilized a restrictive partially blind signature to protect the identities of the owners. The protocol has been proven to preserve identity and location privacy, and to achieve data confidentiality and integrity. Esmalifalak *et al.* [8] and Huang *et al.* [9] considered game theory to protect the smart grid from bad data attacks, and thus improve communication security.

This article discusses the challenges and solutions of V2G security, including its unique security and authentication challenges. Furthermore, in order to secure V2G communications, we propose a new context-aware authentication solution with security and privacy considerations. The remainder of the article is organized as follows. The next section points out major attacks in V2G networks. Then we describe the security challenges in V2G networks. The article goes on to present and discuss our proposed context-aware V2G system framework, where the contexts include battery status and roles. Finally, conclusions are drawn, and future research directions are emphasized.

Security Attacks in V2G Networks

During power and communication interactions in V2G networks, the main security attacks can be classified into three categories: data capturing, data deceiving, and data blocking:

- *Data capturing* considers data collection, interception, and monitoring during wired and wireless communications. For instance, in a replay attack, an illegal LAG may record the exchanged data between a legal BV and a legal LAG, and then repeat or delay the data in an ongoing or a later session. When eavesdropping, a passive attacking node may detect the transmitted data and derive a BV's individual information or determine a communication pattern. Other data capturing attacks (e.g., sniffing, skimming, and traffic analysis) may potentially cause private information disclosure.
- *Data deceiving* includes impersonation or interactive data forgery with the purpose of unauthorized access. For instance, tampering is to modify or delete a BV's valid data to achieve data destruction and corruption; spoofing happens when an illegal LAG may impersonate a legal entity to bypass a BV's verification and obtain a BV's private data; and cloning refers to duplication of a legal BV's or LAG's identity data and rewriting it into an equivalent entity for cheating purposes.
- *Data blocking* (e.g., denial of service [DoS], jamming, and malware) aims at malicious interference in communication channels and backend systems to exhaust the available resources.

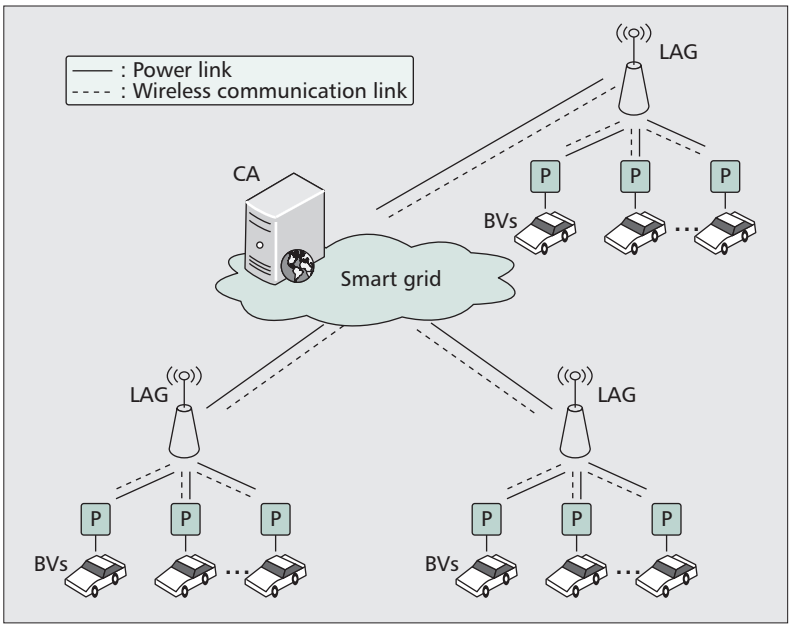

Figure 1. *V2G network architecture.*

Besides these severe security attacks, system vulnerabilities should accordingly be considered in the network components:

- A BV may be equipped with limited system resources (e.g., power, storage, and computational capability), so more full-fledged security algorithms may not be available for advanced protection. Meanwhile, mobility and dynamic participation bring new challenges for identification and authentication while a BV is moving from one area network into another.
- LAGs as power agents are directly related to different power interest groups, and can obtain power and communication data. The data itself may reveal sensitive information from both an individual user and a group of users, which makes LAGs become the main attack target for adversaries.
- The CA is regarded as a secure entity with perfect system resources and security strategies, but it is also confronted with similar security threats (e.g., viruses, worms, and Trojan horses) as those of traditional servers.
- Regarding the communication networks, the main security vulnerabilities are found in the wireless channels, and the interfaces between BVs and LAGs. If these vulnerabilities are exploited, this may cause serious defects in data transmissions and traffic monitoring.

Additionally, computational load and communication overhead also bring challenges when secure solutions are to be designed. Both are very important in optimal performance-security trade-off when the applicability of security solutions is considered.

An adversary should not be able to correlate any two communication sessions, and also should not be able to derive previous or subsequent interrogations in the current session. This means that the interactions among BVs, LAGs, and the CA should be session-constrained.

Security Requirements in V2G Networks

Security Protection Requirements

Security protection provides the basic security requirements to ensure authorized and reliable interactions among legal entities, including data confidentiality, data integrity, access control, forward security, and mutual authentication.

Data confidentiality: The exchanged data (e.g., a BV's power information and a LAG's access query) should be protected against unauthorized access and disclosure. Cryptographic algorithms and anonymous proofs can be applied to ensure that only legal entities can derive proprietary data, and any illegal entity should not be able to deduce unauthorized information.

Data integrity: The exchanged data should be protected against unauthorized modification or destruction, including ensuring data authenticity and behavior non-repudiation. Irreversible functions (e.g., hash functions and keyed hash message authentication codes [HMAC]) and integrity check functions (e.g., cyclic redundancy check [CRC]) can prevent malicious data tampering.

Access control: Legal entities (i.e., LAGs and CA) may be assigned to different access authorities to the same BV. Hierarchical authority management mechanisms should be designed among the legal entities. For instance, a LAG can only obtain basic authentication information to ascertain a BV's identity for connecting to the power grid, but the CA can further derive the needed identity and billing information.

Forward security: An adversary should not be able to correlate any two communication sessions, and also should not be able to derive previous or subsequent interrogations in the current session. This means that the interactions among BVs, LAGs, and the CA should be session-constrained. A unique identifier of the operators (e.g., a pseudo random number, a serial number, or a session identifier) can be introduced to achieve session freshness.

Mutual authentication: BVs and LAGs should authenticate each other before establishing mutual trusting relationships so that any illegal entity should not be able to utilize system resources (e.g., power and information services). In this way, an illegal BV should not be able to access the power grid to steal power resources, and an illegal LAG should not be able to acquire a BV's power status information.

Privacy Preservation Requirements

Privacy preservation protects an individual BV's identity and associated privacy. It aims to ensure that a LAG is not able to correlate a BV's identity with its sensitive information (e.g., battery status, preferences, and location) in its activity cycle, and that private data is not disclosed:

Battery status related privacy: A battery status of a BV can vary (e.g., status of charging [SOC]), and its battery status information should not be detected during connection with the power grid via a LAG. The battery status is a critical parameter in power metering and energy control. Its dynamics indicate the private usage pattern of the owner. As a consequence, it is necessary that only the BV itself and the trusted CA can obtain the BV's detailed battery status information.

Preference related privacy: A BV may have different behavior preferences, and it should not be possible to infer its preference information during its communication with the LAG. For instance, a BV may be asked to discharge power back into the power grid. In this case, the LAG should not be able to ascertain whether the BV accepts or declines the discharging request.

Location related privacy: A BV may move around to different area networks, and its location information should not be correlated with the BV's identity during its connections with LAGs in different networks. In practice, a BV belongs to a specific group and has the corresponding group attributes. For instance, a BV's owner has a subscription with an electricity company, and the BV normally charges power from that electricity company. Here, we can say that the BV is associated with such a company. In such scenarios, a LAG can only obtain a BV's general group attribute without ascertaining its detailed identity information (e.g., real identifier or pseudonym).

A Context-Aware Authentication Solution for V2G Networks

In V2G networks, the interactions among BVs, LAGs, and the power grid (with a built-in CA) take place in different contexts, which have different security and privacy considerations. In this article, the contexts include battery statuses and their roles, as depicted in Fig. 2. The inter-relationships among the contexts are as follows:

- *Battery status awareness* considers the context within which a BV communicates with a LAG during its battery state transitions, including going from the charging state to the fully charged (FC) state, and also transferring from the FC state into the discharging state.
- *Role awareness* considers the context in which a BV connects with a LAG as well as other BVs. The corresponding charging and discharging operations are performed during which the BV may act one of three different roles: energy demand, energy storage, and energy supply.

In V2G scenarios, different communication solutions may be offered. ZigBee recently defined an application layer standard for an energy profile that provides communications primarily related to efficiency, cost, and messaging. The profile intends to support a diversity of devices, including load control devices and electronic vehicles. Wireless sensor networks [10] and vehicular networks [11] can be used to support V2G in intelligent transport systems. Cellular networks support long-range communications, making it a good option for highly mobile BVs. Power line communications can be used for handling message exchanges between BVs and LAGs. It is noteworthy that our main objective is to introduce the importance of contexts in V2G security, and accord-

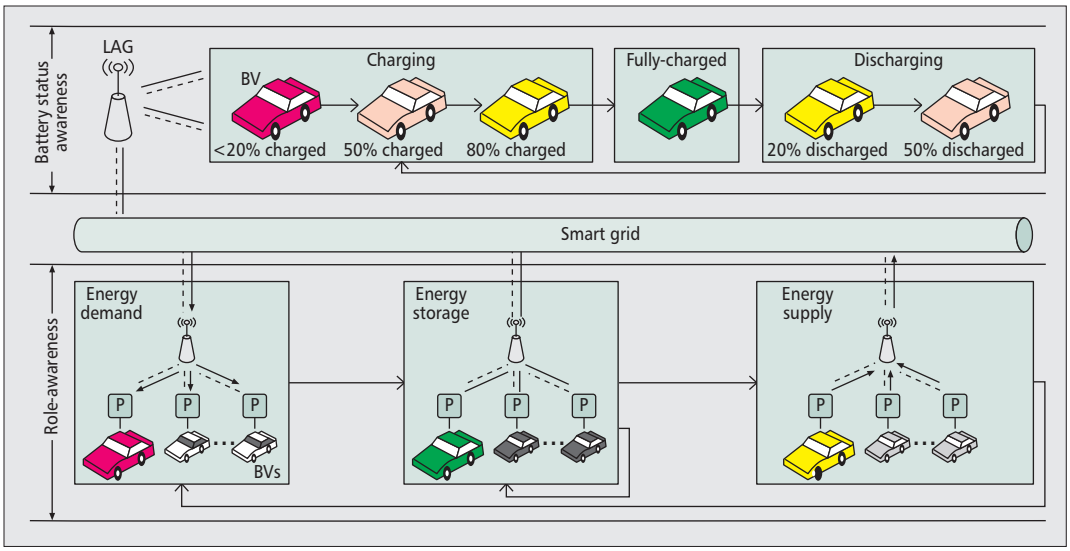

Figure 2. *A context-aware authentication scheme for V2G systems.*

There are different security protection and privacy preservation requirements for BVs in different battery states and during battery state transitions. In such a case it becomes very critical to design an authentication scheme with consideration of battery status.

ingly propose a new context-aware authentication framework for V2G communications in the smart grid. Hence, we need to not limit communications among the interacting entities (including BVs, LAGs, and a CA) to a specific communication network.

The communication process depends on the services provided. A secure communication infrastructure is needed to enable two-way message exchanges among BVs and the grid operation and control centers. For load management problems, communication is mainly performed between BVs and aggregators. The communication is initialized by a BV that needs power charging, followed by various command message exchanges. In this case, the key command messages include power update, power request, charging status, and payment command messages carrying information such as battery status, power pricing, service deadlines, cost information, scheduling information, charging duration, and charging rate.

Battery Status Awareness Context

Figure 2 illustrates the battery state transitions of a BV in a V2G network. In the network, the BV interconnects with a LAG. Both power transmission and communication are established between the BV and the LAG to achieve bidirectional interactions of electricity and information. During the interactions between the BV, LAG, and power grid, the battery may be in one of the three states: charging, FC, or discharging. In the depicted scenario, the BV starts in the charging state with the initial quantity of electricity (QoE) at 20 percent charged battery. Gradually, its QoE increases from 20 to 80 percent, and finally to the FC state. When the power demand from the grid is very high, the fully charged BV may perform discharging to feed the power back into the smart grid. Then the BV is in the discharging state and its QoE decreases. After the discharging operation, the BV may be reconnected to the power grid and perform the charging operation again. This process is repeated during a BV's battery activity cycle.

In the battery status awareness context, there are different security and privacy requirements during the BV's battery state transitions. First, when the BV connects to the power grid from a specific location and attempts to establish communication with the LAG, the BV should be authenticated by the LAG. In this case, the LAG should not be able to obtain the BV's real identity based on the BV's location information. Second, when the BV is in the fully charged state, it may be asked to perform a discharging operation. The BV should have autonomy to decide whether or not to participate in such an operation. In this case, the LAG should not be able to obtain the detailed responses from the BV, in order not to be able to fully deduce behavior related private information. Finally, when the BV completes the discharging operation and turns into the charging state again, it can obtain its own detailed battery status for further billing purposes. However, the LAG should not be able to obtain the BV's power status. Consequently, there are different security protection and privacy preservation requirements for BVs in different battery states and during battery state transitions. In such a case it becomes very critical to design an authentication scheme with consideration of battery status in mind.

The process of a BV connecting to the power grid can be categorized into three battery states, in which the {BV, LAG, CA} perform the following operations:

In the charging state: When a BV connects to a LAG, it attempts to establish bidirectional power and communication interactions with the power grid via the LAG.

In the FC state: If the BV is fully charged, it becomes a potentially available energy source and may feed power back into the power grid. When the BV receives a discharging request, it may accept or decline the request without being monitored.

In the discharging state: When the BV receives a discharging request, it may start to perform discharging and feed its power into the electricity grid. The BV can terminate its dis-

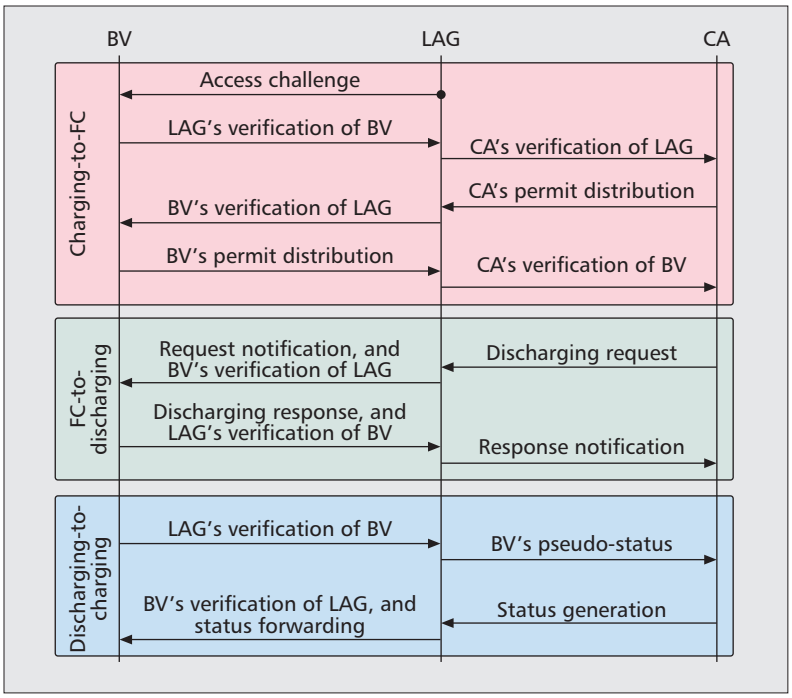

Figure 3. *A battery-aware authentication scheme.*

charging and leave the discharging state if its power level has decreased to a predefined threshold, or the BV leaves the discharging operation because of other private considerations.

Figure 3 shows an authentication scheme for battery state transitions.

Secure Charging-to-FC State Transition — The BV and LAG should perform mutual authentication to ensure the validity and identity of each other. The CA should perform authentication of the BV and LAG to avoid conspiracy attacks. Moreover, the LAG should not disclose the BV's real identity. During this transition, an authentication method works as follows:

- The LAG generates a pseudo-random number, and transmits it as an access challenge to the BV. The BV computes its group attribute identifier based authentication operators, and replies to the LAG for verification.
- If the information from the BV passes the verification, the LAG will transmit its identifier to the CA for verification. In the case in which the LAG is regarded as a legal entity, the CA distributes a permit to the LAG, which grants access authority of the BV to the LAG.
- The LAG forwards the CA's permit to the BV for verification. If the permit passes the verification, the BV will also grant an access permit to the LAG.

Based on the authentication, the LAG can only obtain the BV's group attributes and may not infer its detailed identity, and hence also cannot obtain the BV's detailed location information.

Secure FC-to-Discharging State Transition — The BV itself should have full autonomy to decide whether or not to participate in a discharging operation. This indicates that the BV may first agree to perform a discharging operation and go into the discharging state, then cancel the former positive reply and decline to discharge. Similarly, the BV may first decline the discharging request and stay in the current state, then change its mind and go into the discharging state. Moreover, the BV's response should be anonymously transmitted, and the LAG should not be able to disclose the BV's behavior related privacy. During such a transition, a challenge-response based authentication method could be as follows:

- The CA sends a discharging request to the BV for its power support. The LAG forwards this request to the BV. The LAG also computes the shared secret based authentication operator for the BV's verification.
- If the LAG passes the verification, the BV extracts the discharging response and computes authentication operators for the LAG verifying the BV. If the BV also passes the verification, the LAG will forward the response to the CA.

Based on the authentication, the LAG should not be able to ascertain whether the BV accepts or declines the discharging request, and the LAG should not be able to deduce the BV's preference from the response.

Secure Discharging-to-Charging State Transition — The BV can change its discharging state to the charging state; that is, it may freely perform a charging operation immediately or later. If the BV wants to quit the discharging operation, or its battery is reduced to a certain power level, the BV may want to go into the charging state, depending on the current electricity price and its planned future use of power for travel. The CA may send the BV's detailed power status via the LAG, and the LAG as an intermediary must forward the sensitive data to the BV without obtaining any individual power status for privacy consideration. During discharging-to-charging transition, an authentication method is as follows:

- The BV computes and transmits an authentication operator when it quits discharging, and the LAG performs verification of the BV. If the BV passes this verification, the LAG will transmit the BV's pseudo-status to the CA.
- The CA generates BVs' aggregated status and transmits to the LAG. Meanwhile, the LAG also computes an authentication operator, and transmits it to the BV for verification. If the LAG passes the verification, the BV will derive its own real status for its local battery value.

Based on the authentication, the LAG only obtains the BV's pseudo-status (e.g., wrapped real status), and only the BV itself can deduce its real status and is hence able to preserve the privacy of its battery status.

It is noteworthy that we have considered different mechanisms to defend against major attacks earlier. For the data capturing attack, in addition to ciphertext data transmission, pseudo-random number based access challenges have been presented to avoid session sensitive data capturing. For the data deceiving attack, the private identifier and group attribute identifier have been introduced for verification, and hence any forged data cannot be regarded as valid due to the inconsistency of the pre-shared secrets.

For the data blocking attack, traditional security mechanisms (e.g., firewalls, router control, and antivirus software) can be incorporated to tackle the challenge.

The Role Awareness Context

In a V2G network, a BV may take on different roles, and accordingly have different responsibilities during its interaction with the smart grid. Figure 2 shows the BV's three main roles:

Energy demand: A BV acts as an energy consumer and charges electricity from the power grid. This is the traditional role of the BV, and we call such a BV a load-BV.

Energy storage: A BV acts as an energy storage unit that may potentially provide electricity to the power grid. In this case, we call the BV a storage-BV.

Energy supply: A BV acts as a power generator when it feeds its stored power back into the power grid. In this sense, the BV acts as a small portable power plant (S3P) [12]. Accordingly, we call the BV an S3P-BV.

Regarding a BV's different roles in V2G networks, different security and privacy challenges should be considered. In each role, the same BV has dissimilar privacy concerns and security requirements. It is critical that an anonymous authentication scheme is designed to achieve privacy preservation for BVs, considering role differentiation in the smart grid. Figure 4 shows a ring signature based authentication scheme for the different roles of the BVs.

Load-BV Secure Interaction — A load-BV connects to a LAG as an energy customer to establish both power transmission and communication with the power grid. Before the communications are established, the load-BV and LAG should perform mutual authentication. Moreover, the load-BV should be verified without revealing its sensitive information; therefore, an authentication mechanism is designed for load-BVs in a V2G network. Concretely, the LAG transmits an access challenge to the load-BV, and the load-BV establishes a ring signature as the authentication operator for the LAG's verification; and the LAG also generates a signature for the temporarily gathered BVs. Such an authentication mode provides anonymity in order to ensure that the LAG and other adversaries should not be able to correlate the load-BV's identity with location information.

Storage-BV Secure Interaction — A storage-BV has stored energy, and it may be challenged to participate in a discharging operation. An authentication method is designed for the storage-BV's anonymous response transmission:

- The CA generates a discharging request, and the LAG transmits the request to the storage-BV. The storage-BV signs the discharging response into a ring signature, and transmits it to the LAG for verification.
- If the storage-BV passes the verification, the LAG will derive the response, and forward the response and the storage-BV's authentication operator to the CA for verification. Meanwhile, the LAG computes the shared secret based authentication operator, and transmit it to the CA for verification.

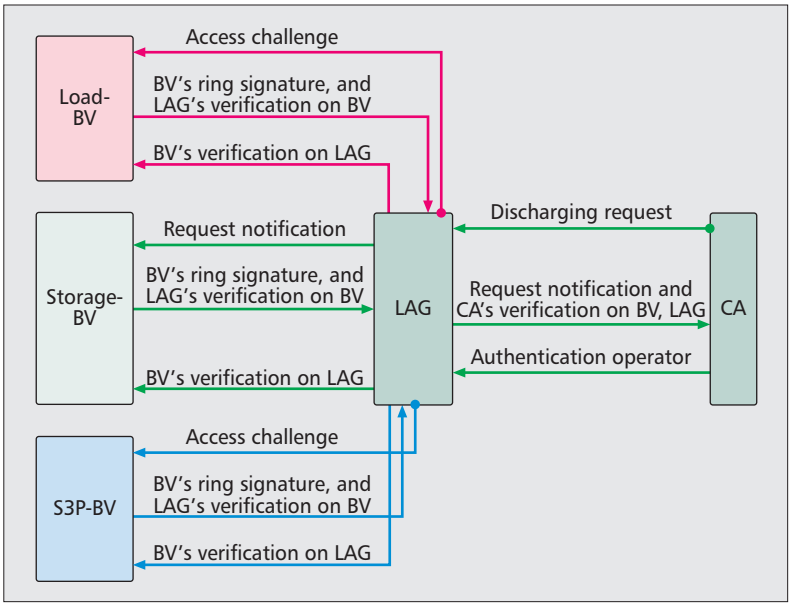

Figure 4. *A role-aware authentication scheme.*

- If both the storage-BV and LAG pass the verifications, the CA will regard them as legal entities and respond with an authentication operator to the LAG. Thereafter, the LAG transmits the encrypted operator to the storage-BV for verification. If the LAG passes the verification, the storage-BV will execute the corresponding operation.

Based on the authentication, the storage-BV establishes ring signatures to ensure anonymity, and the LAG should not be able to determine whether the received nonspecific response (i.e., Agree or Decline) comes from a certain storage-BV.

S3P-BV Secure Interaction — An S3P-BV may perform a discharging operation and feed its power back to the power grid, the neighboring load-BVs, or a local electricity network. During this energy discharging, similar authentication processes as used by the load-BV (including the LAG's access challenge, the BV's ring signature, and the {BV, LAG}'s mutual authentication), can be applied for securing S3P-BVs.

Conclusions and Open Issues

With the smart grid, detailed and improved scheduling of power production and consumption is possible. Battery powered vehicles are used to decrease emissions, but when they connect to the smart grid, important cyber security issues must be addressed. In this article, we have identified such unique security and privacy requirements for V2G networks. We have also presented a context-aware V2G framework, and proposed authentication solutions to address the security challenges during power and communication interactions. The identified security and privacy issues and the proposed solutions indicate that various context considerations are necessary to adequately secure BVs during smart grid interactions.

These challenges and solutions will also spur

Along with the widespread use of BVs, we need to manage a large number of them. This poses significant challenges to authenticate them in a rather short time. Furthermore, there are many more security challenges that need to be addressed due to the unique properties of V2G systems.

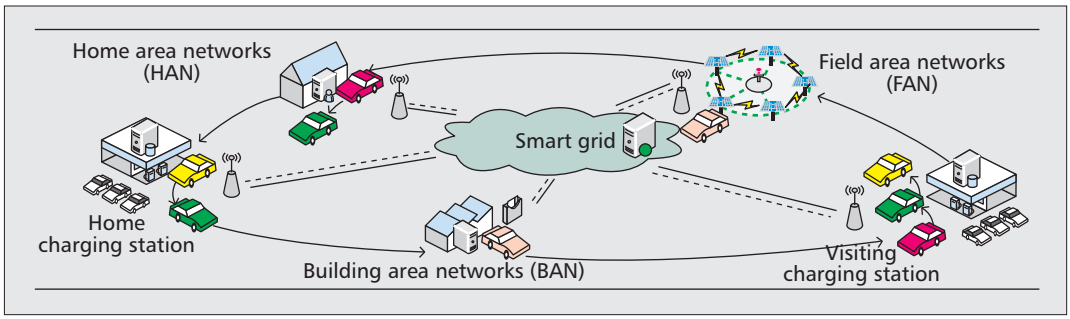

Figure 5. *A BV's complete activity cycle in V2G systems.*

new research efforts and give rise to further developments. For example, along with the widespread use of BVs, we need to manage a large number of them. This poses significat challenges to authenticate them in a rather short time. Furthermore, there are many more security challenges that need to be addressed due to the unique properties of V2G systems.

BVs' Activity Cycle Perspective

From the activity cycle perspective, a BV goes through different area networks with different battery status and diverse roles in the V2G network. Figure 5 shows such a scenario. A BV moves among different networks such as a home area network, a building area network, a field area network, and/or a charging station. The BV temporarily stays in one of these networks and connects to a LAG.

In a home access network (HAN), a BV is parked in its owner's house to perform daily charging operations (e.g., charging in off-work hours), and the corresponding LAG willingly shares its default power and communication access point. On the way from its home to a destination, the BV may become fully discharged. In such a case, it may have to perform charging in a charging station, and hence may turn into the FC state if it is fully charged. After arriving to the destination, in addition to charging, the BV may also perform a discharging operation, and sell the unused battery energy back into the power grid in the local building area network (BAN). Particularly, a unique characteristic of the smart grid is the integration of distributed renewable energy sources (e.g., solar and wind power). Most small renewable energy plants will be used and organized in renewable energy field area networks (FANs), including solar energy and wind farm energy. Accordingly, the BV may perform charging in such a FAN on its way. The complicated interactions among BVs and the smart grid demand fundamental understanding of different contexts and their roles in the design of V2G security solutions.

Vehicle Mobility

Mobility is one of the unique characteristics of V2G networks. A BV can move randomly in a V2G network. Accordingly, a BV may connect to a LAG in either a HAN or a visiting access network:

Home access network: In the case in which the LAG serves as the default power and communication access point for the BV, we say that the BV works in its home access network when it is connected to this LAG.

Visiting access network: In the case that the LAG and the BV have different group attributes, and the BV temporarily connects to this LAG, we say that the BV works in a visiting access network.

Figure 5 shows the home charging station and the visiting charging station. Mobility brings new challenges for identification and authentication during a BV's movement from one area network into another.

In HANs and visiting access networks, a BV is confronted with different authentication requirements. For instance, the BV and LAG may perform more convenient authentication in the HANs than in other visiting access networks. In a HAN, the home LAG provides distributed power services and other advanced data inquiry services for connecting BVs. If a LAG does not recognize a BV, the LAG has a strong demand to verify the BV. In a visiting access network, a BV is not under the jurisdiction of its default LAG, and the LAG only provides the basic power services, without providing additional inquiry services. Considering such challenges, different authentication methods are needed for the home and visiting area networks.

Flexible Discharging Modes

Figure 6 shows two discharging modes for a BV: centralized discharging and distributed discharging. Centralized discharging refers to the mechanism that an S3P-BV feeds its power into the smart grid for centralized energy dispatching. Distributed discharging refers to the mechanism that an S3P-BV feeds its power to the neighboring load-BVs for distributed energy utilization. The former mode is used for the case when there are no load-BVs in the local area network; therefore, the power can be returned into the grid for central management. The latter mode is for the case when there are other load-BVs in the local area network. The discharged electricity will be directly transmitted to the neighboring load-BVs through a LAG for efficiency and cost considerations. In the two discharging modes, the system has different security and privacy requirements. For instance, in the centralized discharging, a LAG cannot correlate an S3P-BV's identity with the energy status. In the distributed discharging, the neighboring load-BVs cannot correlate the S3P-BV's identity with the discharging status, and the S3P-BV or LAG also cannot correlate the neighboring load-BVs' iden-

tities with the charging status. Hence, a new solution is needed when a BV works in different discharging modes.

References

[1] H. Gharavi and R. Ghafurian, "Smart Grid: The Electric Energy System of the Future," *Proc. IEEE*, vol. 99, no. 6, 2011, pp. 917–21.

[2] C. Guille and G. Gross, "A Conceptual Framework for the Vehicle-to-Grid (V2G) Implementation," *Energy Policy*, vol. 37, no. 11, 2009, pp. 4379–90.

[3] D. He *et al.*, "Secure Service Provision in Smart Grid Communications," *IEEE Commun. Mag.*, vol. 50,no. 8, 2012, pp. 53–61.

[4] Z. Yang *et al.*, "P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2012, pp. 697–706.

[5] H. Guo et al., "UBAPV2G: A Unique Batch Authentication Protocol for Vehicle-to-Grid Communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, 2012, pp. 707–14.

[6] B. Vaidya, D. Makrakis, and H. Mouftah, "Security Mechanism for Multi-Domain Vehicle-to-Grid Infrastructure," *Proc. IEEE GLOBECOM 2011*.

[7] H. Tseng, "A Secure and Privacy-Preserving Communication Protocol for V2G Networks," *Proc. IEEE WCNC 2012*.

[10] D. Tacconi *et al.*, "Using Wireless Sensor Networks to Support Intelligent Transportation Systems," *Ad Hoc Networks*, vol. 8, no. 5, 2010, pp. 462–73.

[11] J. Chen *et al.*, "Measuring the Performance of Movement-Assisted Certificate Revocation List Distribution in VANET," *Wiley Wireless Commun. and Mobile Computing*, vol.11, no.7, Nov. 2011, pp. 888–98.

[8] M. Esmalifalak et al., "Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study," *IEEE Trans. Smart Grid*, to appear.

[9] Y. Huang *et al.*, "Bad Data Injection in Smart Grid: Attack and Defense Mechanisms," *IEEE Commun. Mag.*, to appear.

[12] A. Saber and G. Venayagamoorthy, "Efficient Utilization of Renewable Energy Sources by Gridable Vehicles in Cyber-Physical Energy Systems," *IEEE Sys. J.*, vol. 4, no. 3, 2010, pp. 285–94.

Biographies

YAN ZHANG [SM'10] (yanzhang@ieee.org) received a Ph.D. degree from Nanyang Technological University, Singapore. He is working with Simula Research Laboratory, Norway; and he is an adjunct associate professor at the University of Oslo, Norway. He is an Associate Editor or Guest Editor of a number of international journals. He serves as Organizing Committee Chair for many international conferences. His research interests include resource, mobility, spectrum, energy, and data management in wireless communications and networking.

STEIN GJESSING (steing@ifi.uio.no) is a professor of computer science in the Department of Informatics, University of Oslo, and an adjunct researcher at Simula Research Laboratory. He received his Ph.D. degree from the University of Oslo in 1985. He acted as head of the Department of Informatics for four years from 1987. From February 1996 to October 2001 he was the Chairman of the national research program Distributed IT-System, founded by the Research Council of Norway. He participated in three European funded projects: Macrame, Arches, and Ascissa. His current research interests are routing, transport protocols, and wireless networks, including cognitive radio and smart grid applications.

HONG LIU [S'10] (liuhongler@ee.buaa.edu.cn) is currently working toward a Ph.D. degree at the School of Electronic and Information Engineering, Beihang University, China. She focuses on security and privacy issues in radio frequency identification, vehicle-to-grid, and wireless communication networks. Her research interests include authentication protocol design, and security formal modeling and analysis.

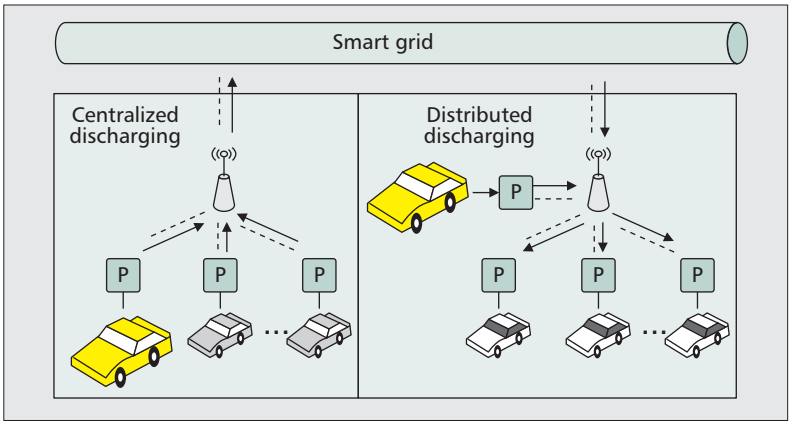

Figure 6. *Centralized discharging and distributed discharging in V2G systems.*

HUANSHENG NING [M'10, SM'13] (ninghuansheng@buaa.edu.cn) received a B.S. degree from Anhui University in 1996 and a Ph.D. degree from Beihang University in 2001. He is an associate professor in the School of Electronic and Information Engineering, Beihang University. His current research focuses on Internet of Things, aviation security, electromagnetic sensing, and computing. He has published more than 50 papers in journals, international conferences/workshops.

LAURENCE T. YANG received his B.E. degree in computer science from Tsinghua University, China, and his Ph.D. degree in computer science from the University of Victoria, Canada. He is a professor in the School of Computer Science and Technology at Huazhong University of Science and Technology, China, and in the Department of Computer Science, St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, and embedded and ubiquitous/pervasive computing. His research is supported by the National Sciences and Engineering Research Council and the Canada Foundation for Innovation.

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] is currently a professor and the associate vice president for graduate studies at Qatar University, Doha. He was the chair of the Computer Science Department at Western Michigan University from 2002 to 2006 and chair of the Computer Science Department at the University of West Florida from 1999 to 2002. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. He received his B.S. (with distinction) and M.S. degrees in electrical engineering, and M.S. and Ph.D. degrees in computer engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, New York. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the Editorial Boards of six technical journals, and is the founder and Editor-in-Chief of the *Wireless Communications and Mobile Computing* journal (Wiley; http://www.interscience.wiley.com/jpages/1530-8669/). He is the author of eight books and more than 300 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. He also served as member, Chair, and General Chair of a number of conferences. He served as Chair of the IEEE Communications Society Wireless Technical Committee and Chair of TAOS Technical Committee. He was an IEEE Computer Society Distinguished Lecturer from 2003 to 2005. He is a Senior Member of ACM.