14 Vehicle-to-Grid Networks
Issues and Challenges

Christos Tsoleridis, Periklis Chatzimisios, and Panayotis Fouliras

CONTENTS

14.1 INTRODUCTION

From an economist's perspective, it would be rather difficult to find the necessary funds in order to build a spinning reserve of energy that could be utilized as a source of electricity. This is where vehicle to grid (V2G) steps in. As electric vehicles (EVs) find their way to massive production, the cost to build such a tank of spinning energy is compensated by the consumers who also gain by allowing

the smart grid to utilize the vehicle's battery when it is parked. This win-win situation has a handful of benefits that should be exploited to the fullest. Therefore, the marriage of several mature technologies such as smart meters/sensors and wireless communication schemes, with the evolution of the power grid could be considered as anticipated by all parties. Currently, governments worldwide attempt to decrease their carbon emissions by increasing the utilization of renewable energy sources. Photovoltaic and wind turbine-based power generators are intermittent energy sources and there could be cases where generation surpasses demand. Storing this surplus into a spinning reserve can later facilitate the reduction of carbon emissions from conventional power generators during peak demand periods. Consumers will also have the opportunity to lease the batteries of their vehicles when not on the road and collect profits that will compensate—if not depreciate—their investment in purchasing the EV.

V2G integration requires the establishment of common standards for smart grids. The charging and discharging process cannot exist without reliable communication between EVs, charging stations, and the smart grid. EVs are designed to move. As a result, the grid will have to organize vehicles into groups managed by base stations, called aggregators, in order to enable effective applications. Consequently, an aggregator will have to be able to communicate with the vehicles and the control center and deliver critical information to the smart grid. There are numerous studies that target toward better medium access control (MAC) protocols to facilitate vehicle-to-infrastructure (V2I), as well as vehicle-to-vehicle (V2V) communications. Moreover, in this networked vehicular environment, additional applications can be implemented, such as safety signaling between the vehicles. The feasibility of communicating dynamically with neighboring vehicles has inspired approaches for better and more resilient vehicular ad hoc networks (VANETs) that, among others, guarantee critical safety information exchange through the novel MAC protocols.

The rest of this chapter is organized as follows. In Section 14.2, we briefly inspect the issue of load management in regard to the application of EV charge and discharge requirements. In Section 14.3, we discuss the interconnection properties of EVs and the smart grid in the wireless domain. Section 14.4 provides an enumeration of MAC protocol considerations that points toward a better supporting layer for the V2G operations. Finally, Section 14.5 concludes our survey by discussing open-research issues and future challenges.

14.2 V2G LOAD MANAGEMENT CONSIDERATIONS

Apart from the recent implementations, there is also an interest in the analysis of how a V2G system should be configured when EV connectivity is taken into account. EVs are considered to be mobile energy-storage units, also called *spinning reserves*, that are distributed and anticipated as the new major factor in energy storage and manipulation. As discussed in Reference 1, worldwide events (e.g., Olympic Games hosting, etc.) were also great chances to invest in preliminary V2G test implementations. The initial objectives of V2G were limited around peak power adjustments, where the batteries of the vehicles store energy in low-load periods and offer that power back to the grid when the demand is overwhelming. This also facilitates

efficiency in the utilization of distributed renewable energy sources as the intermittency of such power generators can be effectively countered.

The main reason that car owners are expected to offer the battery to the grid is that it is expected to be profitable for the owner. Vehicles that are not tied to the owner's profession (e.g., taxi vehicles) are in most cases parked almost the whole day. An average parked time is close to 23 hours per day (Figure 14.1). As a result, there is plenty of time in which the vehicle's battery can be available to the grid as a storage unit. If the demand is high, the grid can draw power from the vehicles to cover the extra demand. The ability to use the EVs as mobile storage units to shift regional load, not only provides social and economic benefits, but also seems to be a better alternative to other ways of energy storage, for example, pump-storage power stations. The charging and discharging times in EVs are in the order of milliseconds as no mechanical components are involved whereas the efficiency is up to 80% according to test data—5% higher than the efficiency of pump-storage stations.

The participation of the vehicle in the V2G service that can provide demand peak shifting would be a win-win schema for both the vehicle owners and the power grid providers. Vehicle owners will be compensated for allowing the grid to make use of the vehicle battery. In turn, the power grid will avoid the expenses of building fixed energy-storage facilities, utilize renewable resources more efficiently, and improve the performance of current power plants.

Moreover, there is a scenario where the EVs assist in frequency regulation by charging according to grid frequency fluctuations. This, appropriately managed charging process is called grid to vehicle (G2V). In this case, the battery is strained less than in the scenario where there is an actual deep charging and discharging cycle. The EV varies its charging power according to received signals and its commitments in order to apply a secondary frequency regulation, known as G2V regulation [2].

FIGURE 14.1 A parked EV linked to a charging station. Oslo, Norway, 2014.

The power reserve in the vehicle can also similarly act to the function of an uninterruptable power source (UPS). Especially in homes equipped with charging points, the EV operates as a voltage source, capable of feeding their loads. This technology begins to be denominated in the literature as vehicle to home (V2H) [3]. The EV, while connected to the grid, can be used to temporarily replace the external grid when there is an outage. In this way, cases like emergency evacuations could be assisted and the reliability of the power supply could be enhanced as short-term power outages can be made invisible to the end user.

In Reference 4, it is stated that despite the fact that a plug-in hybrid electric vehicle (PHEV) can be charged from renewable resources, such as photovoltaic or wind turbine establishments, the intermittency of power generation makes the charging challenging. In PHEV-charging scenarios, the worst case would be the following: the occurrences of critical peak periods (CPPs) to coincide with the time of charging (TOC) of PHEVs. However, simple scheduling could not be effective enough as there is always the need for communication and immediate signal exchange in order to counter problems in real time. This is where the communication technologies fit well into the smart grid system and carry out the process of interactive synchronization between utilities and consumers. Therefore, communications are an integral part for scalable demand-response equilibrium.

Information about the status of assets in current power grid utilities is acquired via the supervisor control and data acquisition (SCADA) system. In Reference 4, the authors propose their communication-based PHEV load management (Co-PLaM) scheme to control the load of the PHEVs. The authors assume that the control points communicate with the utilities including the substation control center (SCC) using a long-range wireless technology such as wireless interoperability for microwave access (WiMAX). The SCC and the smart-charging station communicate by forming a wireless mesh network (WMN) using the IEEE 802.11s standard. In this schema, a simulation of the WMN distribution level was performed and data considering delivery ratio, delay, and jitter were collected. The mathematical analysis of the blocking probability of Co-PLaM was provided and the required additional capacity to supply the PHEVs was presented. The disadvantage of optimization-based approaches is that load, grid capacity, and charging requests are assumed to be known. Nevertheless, when communications are available, the decisions are dynamically determined according to real-time data. This would apply well for the integration of solar energy collectors and wind turbines where the output of generators fluctuates significantly during 24 hours of the day. This is why the utility periodically updates the supplied power thresholds and notifies the SCCs through wireless communications. Since transmission and distribution system conditions can vary due to unforeseen events, if there is information about the grid state in the utilities using the SCADA system, it could be in-sync with the charging stations of the PHEVs. In Co-PLaM, such information is communicated to the SCC that will first query for clearance to access the necessary power load given that it is gracefully available.

The simulation results for the Co-PLaM scheme showed that the energy-provisioning threshold determines the number of maximum PHEVs accepted for charging [4]: thresholds of 200 and 150 kWh correspond to 90 and 100 PHEVs charged during

24 hours, respectively. Furthermore, the system could support prioritized charging in the future for customers who pay more to get their vehicles charged as fast as possible.

Considering the consumer side, if the charging process of the PHEV takes place at the owner's home, the charging could be coordinated with other in-home activities to avoid exceeding a certain level of overall consumption.

The selected flavor of IEEE 802.11s uses a hybrid wireless mesh protocol (HWMP) that combines on demand and proactive-routing algorithms. The MAC layer is implemented based on the enhanced distributed channel access (EDCA) standardized in IEEE 802.11e [5].

The peak of power demand for commercially available PHEVs is between 1.8 and 16.8 kW. Charging implementations include fixed-demand cases or charging cycles that draw more energy for the first period of charging and then lower ones to be able to charge more when there is little available time for charging. For example, the battery of a Tesla Roadster can be charged within 4 hours at a peak power level of 16.8 kW. It should be noted that currently, Tesla Motors is also investigating the possibility of exchanging batteries rather than charging them in the charging stations. A prototype changing the battery within 90 seconds has been already demonstrated. However, the exchange process and how the replacement will be handled are still under testing [6].

14.3 V2G INTERCONNECTION SPECIFICS

The V2G applications can be placed within the map of communication requirements of the smart grid. In Reference 7, they are classified as neighborhood area network (NAN) applications that are the middle class between the home area network and wide-area network application classes (Figure 14.2). Typical functions include the delivery of pricing information from power utilities to EVs and EVs can provide information about the status of the battery charge level back to the utilities. Typical data sizes are expected to be 255 and 100 bytes, respectively, while latency should be below 15 seconds and reliability over 98%.

According to Reference 8, two types of wireless communications are required for a V2G system (Figure 14.3):

- The communication scheme between the aggregator and the control center realized through IEEE 802.16.d and commercialized as WiMAX.
- The communication scheme between the aggregator and the EVs realized through IEEE 802.11p wireless access for vehicular environment (WAVE).

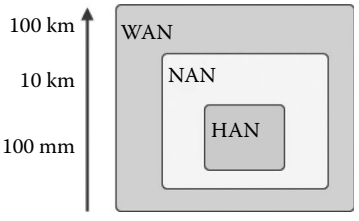

FIGURE 14.2 Network area hierarchy ranges in the smart grid.

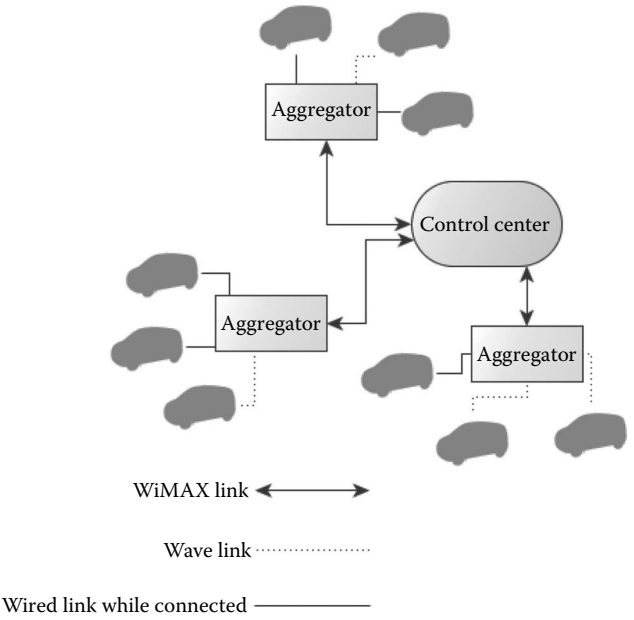

FIGURE 14.3 V2G communication scheme.

Parking locations, whether at home or at underground parking lots, etc., would have to provide bidirectional connectivity to the power grid, as well as two-way communication to the aggregators [9]. The latter unifies many vehicles and provides a single interface for a large group of vehicles. Aggregators are required to communicate with the smart grid operator, called the control center. Concentrating information to a small number of service providers who aggregate EV capacity, sets the control center workload to feasible levels. Thus, the aggregators handle the customer interfacing, metering, and billing, and leave higher-level processes for the control center.

Considering the wireless protocols, the authors of Reference 8 selected the WiMAX communications standard for communication between the control center and the aggregators and the 802.11p for aggregator-to-EVs communication. If the control center determines a deficit in power coverage, a message can be dispatched to the aggregators that can be forwarded to the EVs. The message can be delivered to both parked and moving vehicles, so that their owners have the option to connect to the grid. The security concerns of this information exchange require source authentication, message integrity, replay attack resistance, and privacy protection.

The WiMAX was initially designed for cases with line of sight (LOS) within the 10–66 GHz frequency band. The 802.16a amendment specified working bands between 2 and 11 GHz that partially enable non-LOS transmissions. The WiMAX standard defines the air interface that includes MAC and physical (PHY) layers.

There are three different PHYs available that provide end-to-end implementation along with the MAC layer.

- A single-carrier (SC)-modulated air interface.
- A 256-point fast Fourier transform (FFT) orthogonal frequency-division multiplexing (OFDM), multiplexing scheme.
- A 2048-point FFT OFDM scheme.

The 802.11p WAVE defines modifications to IEEE 802.11 for dedicated short-range communication (DSRC) between the vehicles. There are enhancements that could be derived from the standard for transportation safety such as collision avoidance and emergency breaking.

In Reference 8, the authors developed two simulation models in MATLAB® Simulink®, one for each of the communication protocols used. For the aggregator to EV, the LOS and non-LOS cases were inspected separately due to different radio propagation characteristics. For the LOS case, the two-ray path loss model was adopted to determine the received signal power level. Low spectral efficiency modulation schemes, such as binary phase-shift keying (BPSK) and quadrature phase-shift keying (QPSK), which carry less information (bits) per symbol, require lower energy per bit and can work in a higher noise floor environment since they are less vulnerable to bit errors. Simulations show a higher packet error rate for higher-modulation schemes.

Similarly to the vehicular case, the WiMAX requires high energy per bit over noise power spectral density, which means that more energy is required for each bit transfer. The distance between the two peers was set to 1000 m and the conclusion was that BPSK modulation is the most robust as expected. Increasing the code rate translates to a higher packet error rate. For the non-LOS path, it is evident that the performance degrades proportionally to the distance and message signal increases.

In Reference 10, there is a discussion about the V2G integration and an overview of the current working international joint ISO/IEC standardization of the vehicle-to-grid communication interface (V2G CI). Efforts are made to take into account the full potential of EVs and any possible use case to be exploited as it is expected that EVs will be a commonplace for everyone. For instance, the first use case dictates charging of the EVs at home, which seems a trivial process, but if we look closely at the nature of an EV's power needs, there is no similar appliance currently within a typical household. The capacity of a 30-kWh EV is able to power a four-person household for a few days. Moreover, the EV is expected to recharge overnight. Billing is also different as electric vehicle supply equipment (EVSE) is shared by many consumers. Hence, there is no one-to-one relation that ties the consumer of the power grid with the corresponding consumption.

In this context of information exchange between the EV and the grid, the authors of Reference 10 provide an overview of the message structure and message patterns as defined in V2G CI working draft of ISO/IEC 151180-2. Messages are exchanged over an IPv6 link based on power-line communication (PLC) carrier medium. A suggested encoding layout for the messages is the binary extensible markup language

(XML) that provides the loose restrictions of XML along with a binary serialization to avoid an unnecessary overhead. Recent evaluations imply that the usage of W3C's efficient XML interchange (EXI) [11] fits the realization of the V2G-based interaction signaling. The types of messages between EV and EVSE can be differentiated as plugging-in, service discovery, authorization, power discovery, power request, payment, charging cycles, and unplugging.

In Reference 12, the authors point out that EVs are a significant capital investment that can facilitate in renewable and, in most cases, intermittent energy sources through closely attended integration. It is also discussed that the IEEE 802.15.4 (Zigbee) protocol, by designing a low-power (<1 mW) connectivity implementation, can fit well for metering and signaling communications for plug-in EVs (PEVs). Communication-driven management of EV charging/discharging behavior is a prerequisite to scaled EV adoption, since the unattended and opportunistic charging of EVs adds up to the inefficient overall load of power consumption even during peak hours. Consequently, in order to meet the power requirements of EV transportation as a mainstream means of transportation, the load has to be shifted to off-peak hours or additional power has to be generated. By simulating the interaction between PHEVs and the power grid, the authors of Reference 12 conclude that utilities may be able to reduce the extra capacity needed to serve PHEVs by implementing a low-throughput communication system.

14.4 THE MAC PROTOCOLS

Mobile ad hoc networks (MANETs) where nodes self-configure themselves and interact without using fixed infrastructures or centralized administration are discussed in Reference 13. Such network topologies do not allow more than one transmitting terminal at a given time for each channel. In order to effectively share the medium, different existing MAC protocols suitable for VANETs were tested.

In the MANET domain, one of the first MAC protocols to counter the shared-medium problems was ALOHA with a random access-oriented approach and S-ALOHA. The carrier sense multiple access (CSMA) protocol was also examined, concluding that the main weaknesses are the hidden- and exposed-terminals issues. The hidden-terminal problem occurs when a terminal starts transmitting while failing to detect another terminal that also transmits because it is out of range. The exposed-terminal problem occurs when a transmission is falsely blocked, because the transmitter senses a neighbor-transmitting node that will actually not interfere with the transmission. Multiple access with collision avoidance (MACA) introduced the request-to-send (RTS) and clear-to-send (CTS) mechanisms to counter the hidden-terminal problem by agreeing with the receiver on the transmission.

Nevertheless, there are cases where the exposed-terminal problem does occur. MACA wireless did counter the exposed-terminal issue by adding data-sending and acknowledgment packets with regard to RTS and CTS packets. The busy tone multiple access (BTMA) MAC protocol proposed a new way to counter the hidden-terminal problem by splitting the channel transmission into two channels: a data and control channel (CCH). The latter is used to transmit the busy tone. When a node

receives the busy tone, it retransmits the signal in order to notify its neighbors who might be out of the transmission radius of the original signal [13].

Other ways to split the medium include division in terms of time. Time division multiple access (TDMA)-based methods employ fixed time frames where each frame is further divided into several slots. The five-phase reservation protocol (FPRP) was the first-proposed TDMA protocol in which the medium is divided into information frames (IFs) to send data and reservation frames (RFs) for reservations.

In frequency division multiple access (FDMA), the medium is slotted in terms of frequencies in order for multiple stations to transmit concurrently. Other MAC proposals can be applied in each frequency channel such as memorized carrier sense multiple access (MCSMA) where CSMA is used in each channel.

In code division multiple access (CDMA)-based protocols, several orthogonal codes are available and each node uses a code to encrypt messages before transmission. For example, in multicode MAC (MC MAC), several codes are used with one of the codes reserved for control packet transmissions.

VANETs are destined to adapt MANET-qualified protocols into use cases where peers are vehicles that try to transmit and receive from other vehicles or infrastructures. Different approaches are considered to achieve reconciliation between performance and reliability in VANETs (Figure 14.4):

1. In the WAVEs protocol that is referred as well as IEEE 802.11p, the PHY and MAC layers are tuned for VANETs. By using OFDM, V2V, and V2I, connections are possible over distances up to 1000 m. High speed between

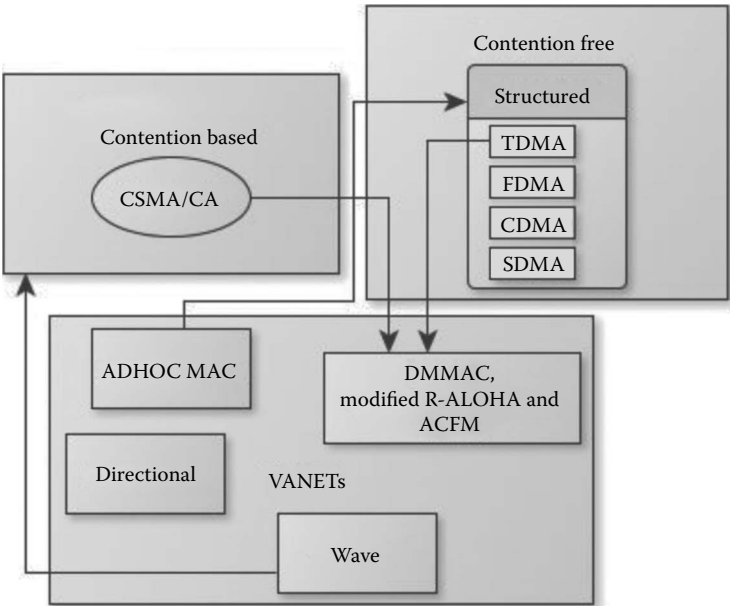

FIGURE 14.4 Overview of the discussed MAC properties.

peers is taken into account in which fast multipath-fading scenarios are countered with the OFDM technology.

2. ADHOC MAC is an MAC protocol of the European project CarTALK2000 (FleetNET has been the follow-up) as a means of solving VANET communication issues. The selected structure is a slotted MAC frame, independent from the PHY layer, through the use of a dynamic TDMA mechanism that could be adapted to the universal mobile telecommunications system (UMTS) terrestrial radio access time division duplex (ULTRA-TDD). The reliable R-Aloha (RR-ALOHA) protocol used in ADHOC MAC, employs the dynamic TDMA mechanism by having each car select a basic channel (BCH), which, in turn, is a time slot periodically repeated in consecutive frames. In the implementation, each peer sends its frame information on the BCH, containing a vector that indicates statuses sensed in the previous frame.
3. Directional antenna transmission is also a way of bypassing MAC issues in VANETs. The vehicles move within the allowed routes of the motorway network and, therefore, directional antennas could certainly help in reducing collisions in cases of parallel neighboring vehicular traffic. Having multiple antennas allows the node to block the antenna that receives an RTS transmission.

The authors of Reference 13 note as the main weakness of the 802.11 MAC, the drawbacks in throughput caused by the CSMA/CA mechanism that cannot guarantee a deterministic upper bound on the channel access delay. On the other hand, the ADHOC MAC does not use the medium efficiently and the number of vehicles in the same broadcast domain cannot be greater than the number of slots in the time frame. Finally, the directional-antenna-based MAC does improve network throughput by fighting collisions but at a cost: several antennas are required in practice, making the solution more expensive than single-antenna implementations.

In Reference 14, the authors propose a dedicated multichannel MAC protocol, called DMMAC, which uses an adaptive broadcasting mechanism in order to provide collision-free and delay-bounded transmissions for safety applications under various traffic conditions. In this approach for VANET environments, a hybrid channel access mechanism is exploited in order to deliver both the advantages of TDMA and CSMA/CA. All vehicles are equipped with a single half-duplex radio to avoid cross-channel interference from multiple radios for each node.

The MAC protocol for VANETs is required to be reliable and efficient as all MAC protocols, but with the specialty of the highly dynamic network topology of moving vehicles with regard to different kinds of quality of service (QoS). In 1999, the U.S. Federal Communications Commission (FCC) allocated seven 10-MHz channels in the 5.9-GHz band, including the six service channels (SCHs) and one CCH. This layout, along with the nature of the vehicular network environment, which cannot follow typical channel reuse techniques, has led to studies for multichannel MAC protocols for higher throughput and network latency. Dividing the band according to the regional data would not make any sense since the key factor in this case is proximity among vehicles. The authors of Reference 13 also argue about the insufficient

scheme of the current WAVE MAC with the contention-based channel access implementation, which cannot guarantee the QoS of safety, and other real-time applications in high-density scenarios.

In the DMMAC architecture, the channel coordination is similar to WAVE MAC. Access time is equally divided into sync intervals with each one consisting of a CCH interval (CCHI) and an SCH interval (SCHI) of the same length. In DMMAC, there is further division of the CCHI into an adaptive broadcast frame (ABF) and a contention-based reservation period (CRP). ABFs are, by design, suitable to deliver safety messages as they are set to inform the sender that they were delivered, while also informing about the outcome of a transmission. The number of time slots within each ABF is called the ABF length (ABFL). This length is not statically specified for the whole network. However, there is a set of maximum and minimum values predefined in the system and each vehicle can adjust its ABFL in every CCHI, accordingly. These adjustments, along with other details of adaptive broadcasting, are presented in the adaptive broadcasting implementation protocol (ABIP), which is a set of rules for regulating the access behaviors of the vehicles in the ABF, how to reserve a slot as BCH, adapt the ABFL, and determine whether to add virtual slots after the end of the ABF. The ABIP can provide every vehicle a contention-free opportunity to transmit. However, vehicles still need to contend in order to reserve a slot when there are many vehicles that want to reserve the BCH simultaneously.

By using CSMA/CA, the CRP provides a means for vehicles to make reservations for non-safety-related applications. The CRP also depends on the ABFL of the vehicle. In order to prevent potential collisions, some vehicles have additional slots named virtual slots. Generally, a pair of vehicles need to exchange three types of packets: CRP-REQ, CRP-RES, and CRP-ACK. SCHI also divides the channel access time into equal-duration slots and all slots on the same channel are grouped into one nonsafety application frame (NSAF). All NSAFs in one SCHI can be reserved during the CRP for collision-free transmissions of non-safety-related data.

The comparison of results of DMMAC with WAVE MAC in terms of safety packet delivery performance showed that DMMAC decreases slightly, whereas WAVE MAC grows steadily worse as the competition between nodes to occupy the medium increases.

As discussed in Reference 15, the specific area of VANET still faces significant challenges in the design of reliable and robust MAC protocols for V2V communications. VANETs are designed to provide coverage within 1000-m radius with roadside units (RSUs) and other vehicles, while traveling at relative speeds up to 200 km/h, regardless of the surrounding environment. Apart from the information considering V2G integration, there is safety-related information that will be incorporated into predefined basic signaling schemes, such as lane change assistance, cooperative forward incident warning, intersection collision avoidance, and emergency or incident warning.

It is evident that an MAC protocol designed for infotainment has to take different things into account compared to an MAC protocol designed for safety signaling. However, both these cases are a requirement in VANETs since one complements the other in order to be presented as a product with successful embodiment to the car

industry, be it electric or conventional. Safety messages are short and are required to be delivered as soon and as reliably as possible, while infotainment services overtake wider data load with less regard to low-latency requirements. Furthermore, these two services are also opposite in the sense that one tries to increase the driver's awareness for potential threats, whereas the other increases potential sources of distraction.

Within a broadcast domain, the peer-granted access to occupy the PHY medium is determined by the MAC layer. A categorization of the MAC mechanisms in terms of access approach could be as either contention based or contention free. The former is based on carrier sensing and backing off until the next attempt to transmit; the latter divides access into time slots and uses synchronization schemes. It is, however, possible to have a mixture of the two methodologies in the same implementation.

A basic distinction between MAC mechanisms would also be the point of control of the medium access. Medium access can vary in terms of methodology. It can be completely random and the nodes would try to access the medium with little or no coordination. On the other hand, there are more structured approaches where there are certain time slots, or certain frequency channels allocated according to prearranged layouts. More specifically, for the structured approaches, there are four fundamental techniques that can be tweaked or combined in various ways. These are the TDMA, the FDMA, the CDMA, and the space division multiple access (SDMA).

Contention-based methods tend to better utilize the medium and consume less energy with less coordination required. There is also more resilience to network changes. On the other hand, in scenarios with high traffic load and many peers contesting for a chance to transmit, the performance of contention-based implementations deteriorates significantly due to increased collisions. Contention-free MAC methods can restrict access delays to certain bounds, QoS can be guaranteed, and the overall performance is better under increased network traffic load. Such methods are considered more reliable and are expected to utilize the channel better. There is, however, more coordination needed—especially in cases where the network is rapidly changing and portions need to be reallocated frequently.

14.5 CHALLENGES

14.5.1 Technical Aspect Challenges

In this section, we present a selection of technical challenges, outlined in Table 14.1.

14.5.1.1 PHY Layer

Challenges that need to be taken into account in the PHY layer include the Doppler effect, multipath fading, adjacent channel interference, and interference from the other RF sources. In addition, the mobility between nodes in V2V or V2I makes things even more challenging as the surroundings constantly change. Hence, assumptions for the effective guard interval length in OFDM transmissions are more complicated. Link PHY properties vary continuously.

TABLE 14.1
Technical Challenges

	Technical Aspect Challenges
A.	PHY layer: Doppler effect, multipath fading, adjacent interference, interference from other sources, and mobility between peers
B.	MAC metrics relative to VANETs with mobile peers: Access delay, payload delivery delay, throughput, overhead, access fairness, probability of successful delivery, and network stabilization time
C.	MAC layer: Hidden terminal, dynamic nature of VANETs, and QoS issues such as time-of-delivery restrictions for safety signaling
D.	Specific requirements for V2G communication: Latency, bandwidth, and effective radius. Required information from EV to the aggregator and information available to the EV
E.	Security threats and requirements to be met in a smart EV-charging service. Authentication protocol: Safe integration with the current power grid information systems
F.	Routing protocol challenges related to key factors of VANETs
G.	Wireless charging: On-the-fly charging, wireless charging efficiency, effective distance fine-tuning, and ease of use

14.5.1.2 MAC Metrics Relative to VANETs

Since VANETs are distinguished from other ad hoc networks due to high node mobility [15], suitable metrics of evaluation for the MAC layer would be the maximum medium access delay, payload delivery delay, throughput, overhead, access fairness, probability of successful delivery, and network stabilization time. The latter is very important for VANETs. One of the main objectives is a cost-effective and scalable technology that minimizes the time of establishing connections and access delays to the underlying wireless medium for V2V or V2G scenarios. There is no resemblance to the cellular Internet connectivity that is inherently infrastructure based.

14.5.1.3 MAC Layer

At the MAC layer, the challenges for VANETs include the hidden terminal, the dynamic nature of VANETs, the scalability requirements, and the great divergence in the requirements of applications designed for the vehicular environment. Single-radio implementations are unable to transmit and receive simultaneously, leading to indirect collision detection. Nodes in a VANET are inherently mobile. Therefore, the MAC layer should be optimized for continuous disconnects and roaming between RSUs and on-board units (OBUs) of other vehicles. Moreover, in V2I schemes, the RSU can act as a coordinator for centralized MAC methods, whereas in pure V2V schemes, there is no such option for access management and coordination among allocated channels. Similarly, the QoS requirements are difficult to meet, especially for safety messages, where the objective is to guarantee message delivery within the time frame that the information will be valid and useful.

14.5.1.4 Requirements for V2G Communication

As stated in Reference 16, the entities that are part of the V2G architecture require very specific communication platforms in terms of latency, bandwidth, and effective radius. Furthermore, the security of the information to be exchanged is also vital as attacks can produce severe problems to power distribution. According to Reference 16, the typical information that the power aggregator needs from EVs includes the ID of the EV, battery voltage, battery chemistry type, temperature, charging profile (how much available), driving habit, etc. On the other hand, the OBU would be able to obtain information about secure user identification, current grid frequency, charging station(s) location (GPS), metering data for actual power flow (demand/supply), corresponding billing rates, etc.

14.5.1.5 Security Threats and Authentication Protocol

The opportunities of attackers targeting smart EVs are enumerated in References 17 and 18. Possible threats include impersonation, tampering with communication messages, eavesdropping, denial of service (DoS), privacy breaches, and disputes. The authors propose actions to counter these threats by establishing

- Stronger entity authentication
- Enhanced message authenticity checks
- Centralized and role-based access control authorization
- Symmetric or/and public key encryption for confidentiality assurance
- Nonrepudiation to increase the level of trust
- Measures to ensure maximum possible availability for key services in order to withstand DoS attacks
- Anonymity and nonlinkability (privacy preservation) by incorporating a trusted third party

A different distinction of the security concerns of an EV is enumerated in Reference 19, after suggesting that such a vehicle can—from now on—be considered as a fully connected network device:

1. Data: The information exchanged between the vehicle and the grid needs to be protected from packet sniffing and resilient to replay attacks. Furthermore, the already-stored data must be immune to attacks, such as structured query language (SQL) injection, etc.
2. Communication network: In the context of using the ZigBee protocol for connections between the EV and the utility, all weaknesses already addressed need to be amended before deployment. This applies to any wireless protocol potentially involved.
3. Infrastructure: Since EVs will be utilized as energy-storage assets for distributed energy resources (DERs), every device that acts as a mediator along with the EV itself will have to be free of malicious software, viruses, and vulnerable or exploitable network services. By verifying the sanity of every component of the involved infrastructure, a considerable part of the possible threats for the grid can stay under control.

4. Firmware and software: A contemporary vehicle already has several electronic control units (ECUs) controlling the functionality of various in-vehicle systems. This firmware must be updated assuring that the received update comes from a trusted and authorized source. The maintenance and repair technicians or even the users themselves must also be restricted from tampering with these processes.

As a result, the authentication protocol is obliged to meet special challenges related to EVs, such as large overhead and latency that are crucial for secure wireless communications between fast-moving nodes. In this context, Chia et al. [20] focused their research and deployment to cyber security, EV charging and telematics for EVs, and the smart grid in a dense urban city environment such as Singapore. The deliverables of the developed smart grid cyber security architecture for the EV-charging infrastructure were assurance of the correct information for EV-charging coordination, secure payment and transaction integrity, safe integration with the power grid information system in the midst of possible new attacks, and minimization of exposure to potential risks for intelligent electronic devices within the smart grid. Furthermore, in Reference 21, the authors identify unique security challenges in an EV's different battery states. Privacy preservation aims at decoupling identities from their sensitive information. Their proposed battery status-aware authentication scheme hides each EV's identity from disclosing location-related information and introduces challenge–response to achieve dynamic response without revealing the user's related privacy. Another privacy-preserving communication protocol for V2G networks is proposed by Tseng in Reference 22. In this attempt, a restrictive partially blind signature is utilized to protect the identities of the EV owners. Blind signatures involve signing without revealing the content of the message to the signer. It is also noted that the proposal is designed in a way to simplify the certificate management infrastructure that as noted in Reference 23, can reach a considerable amount of workload required in a smart grid.

Khurana et al. [23] note that the smart grid is poised to transform a centralized and producer-controlled network to a decentralized and consumer-interactive network. This dictates very specific requirements in terms of trust; for example, each user is accessing accurate data created by the right device, at the expected location and proper time, by an expected protocol, and that the data were not tampered with. Another interesting conclusion was that the requirements for effective cyber security solutions contain the parameter that power availability is more important to most users than power flows information confidentiality. Moreover, the transmission substations authentication and encryption requirements involve cases with multicast messages that must be delivered in less than 4 milliseconds. This implies that efficient authentication algorithms will have to minimize the computational cost and that packet buffering should be avoided so that presented requests are processed immediately.

Toward this objective, Guo et al. [24] proposed a batch authentication protocol called UBAPV2G that tried to deliver reduction of authentication delay, less computational cost, and less communication traffic versus the standard one-by-one authentication scheme. However, in Reference 25, it was shown that this approach created

vulnerable use cases in which either the vehicle or the aggregator can generate a collection of bogus signatures that satisfy the batch verification criterion, that is, forgery attacks. Furthermore, in Reference 26, the authors propose a multidomain network architecture for V2G infrastructure that includes hybrid public key infrastructure (PKI), using hierarchical and peer-to-peer implicit cross-certifications. Their simulation results showed significant reduction in the validation duration when compared to the hybrid PKI scheme using explicit certificates.

14.5.1.6 Routing Protocols

Despite the fact that the routing requirements in VANETs are well defined and exploited by the research community, there are several challenges to be ventured, especially if low-cost and low-power consumption networks are to be used [27]. These challenges are related to key factors of VANETs' mobility already addressed in this chapter and enumerated in Reference 28. In References 29 and 30, there are detailed classifications and discussions of the current routing protocols for VANETs whereas in Reference 31, future research directions for routing protocols in a smart grid, in general, are proposed. The addressed topics include QoS architecture, secure routing, secure and QoS-aware routing, hybrid routing using PLC and wireless communication, cross-layer routing via multichannels and multiple-input–multiple-output (MIMO) antennas, scalable routing, simulation tools and test beds for routing, standardization and interoperability in routing, and multicast routing.

14.5.1.7 Wireless Charging

Chia et al. [20] also addressed the challenge of a successful wireless EV-charging scheme. They concluded that ideas such as on-the-fly charging while the vehicle is traveling along charging lanes or while waiting at traffic lights can become a reality through wireless charging. A solution to achieve high efficiency (>90%) of wireless power transfer over distances of several centimeters to meters makes use of a phenomenon called magnetic resonance coupling. This phenomenon is a special case of inductive coupling, taking place when the transmitting and receiving coils, together with their matching circuits, are made to resonate at a specific power transmission frequency and at a specific distance. The challenge involves successful integration in the actual charging point because small deviations in the distance between the coils results in severe deterioration in efficiency. Current implementations try to fine-tune to the optimum frequency after the vehicle is parked. Otherwise, the driver of the vehicle would be required to place it in a very specific position that is a difficult task. This process would naturally degrade the user's convenience.

14.5.2 Macroscopic Integration-Related Challenges

In the second part of this section, there is an overview of macroscopic and integration-related challenges as shown in Table 14.2.

14.5.2.1 V2G Communications Security and Reliability

In every EV-charging planning context, even in battery swapping, the efficiency of the communication schema that delivers critical information about energy availability or

TABLE 14.2
Macroscopic Challenges

	Macroscopic Integration-Related Challenges
A.	Importance of secure communications in V2G even in battery-swapping cases, battery degradation, and investment costs
B.	Modeling objectives of EVs and the household: Load variance, cost-efficiency optimization, and cost-emission minimization
C.	GEVs: Grouping architecture and optimal sizing of GEVs
D.	Integration software to couple EVs and other active V2G entities along with DERs and the rest of the smart grid

battery throughout, is a fundamental factor that will greatly improve or worsen user experience. Challenges to a V2G transition include battery technology evolution and the high initial costs compared to conventional vehicles. Limitations to using the PEV for V2G will likely be related to implementing assured and secure communications, particularly between an aggregator and a large number of PEVs.

Security issues are important in the communication network at home as well as while visiting public-charging facilities [32]. An additional issue is that the distribution grid has not been designed for bidirectional energy flow; this tends to limit the service capabilities of V2G devices. Conversely, the implementation of fully bidirectional communications in the V2G infrastructure (and the smart grid, in general) introduces new possible vulnerabilities. As discussed in Reference 33, attacks such as DoS and price manipulation can prevent the owner of an EV to determine a real electricity price that can result in suboptimal decisions on charging/discharging planning. In their work, a policy of charging is proposed with respect to resiliency under price information attacks.

Battery degradation issues [34,35] as well as investment costs and energy losses [36] are also important research areas. According to Reference 37, if PEVs are to become the preferred vehicles within the United Kingdom, a significant investment in electrical networks will be required. Moreover, each V2G entity can have multiple roles within the system according to the current function performed: energy demand, energy storage, or energy supply. This further complicates the security considerations to be met as shown in Reference 38 where the authors also propose a role-dependent scheme to preserve each entity's privacy.

14.5.2.2 V2G Modeling Objectives

In the literature, the issue of successfully profiling EV energy that needs incorporation into the contemporary household is well addressed. When EVs are connected to the power grid for charging and/or discharging, they become griddable EVs (GEVs) [39]. GEVs are considered to be primarily connected to the home (V2H) and then considered for V2V and V2G. This indicates that the big picture includes all these models. The modeling of V2H, V2V, and V2G systems should be based on the objectives and their constraints. General objectives are load variance minimization, cost minimization, cost-efficiency optimization, cost-emission minimization, power loss

minimization, load shift and peak load reduction, and reactive power compensation. The demand-response management problem is defined in a scaled view of those issues. Case studies and research projects indicate that the embodiment of innovative technologies is required. Such enabling technologies include smart meters with advanced-metering infrastructure (AMI), home energy controllers, energy management systems (EMSs), and wired and wireless communication systems [40].

Moreover, in Reference 41, there is work toward the adjusting of the load uncertainty in the presence of PEVs. Given that V2G technology is potentially a new renewable energy resource, it can be utilized in order to decrease operational cost.

14.5.2.3 GEVs Architecture

Apart from PHY connections with the power grid, the GEV has other interactions with the grid for V2H, V2V, and V2G operations: information and communication. The V2G operation requires a reliable and secure two-way communication network, enabling message exchanges between the GEVs and the power grid. There are numerous suggestions for V2G communication networks such as References 24, 39, and 42. The diversity and flexibility of V2G communication networks also pose challenges to the architecture. A direct V2G control system is the simplest architecture, where the GEVs are directly supervised by the grid operator; but the large number of GEVs penetrated in the grid increases the computation load of the grid operator tremendously; this led to the adoption of indirect V2G architectures. Here, as already stated, the third entity (aggregator) is involved in reducing the workload of the grid operator. Consequently, the issue of optimal GEV aggregation sizing arises, in which the parameters to be determined involve communication platform limitations, as well as coordination computation load limitations.

14.5.2.4 Integration Software

A nonnegligible aspect of V2G challenges includes the high-level mechanics that will enable its full potential. Toward that goal, the VOLTTRON platform [43] provides an agent execution environment to fulfill the strict requirements of V2G applications such as coordinating EV charging with home energy usage. Another interesting approach is considered in Reference 44, where the authors show that a virtual power plant (VPP) that integrates V2G-enabled EVs has many similarities with instant messaging (IM) and voice over IP (VoIP) in terms of communication patterns. The move to propose the use of session initiation protocol (SIP), a well-established standard, in order to transmit status, trip information, and charging process control signals between EVs and the VPP. Finally, there is a discussion of a web services-oriented approach [45] as a means to interconnect every V2G-integrated device. Devices profile for web services (DPWSs) provides a generic middleware and profile for embedded devices based on web service technologies. It is closely related to universal plug and play (UPnP) [46]. Both offer nearly the same functionality to the application layer: addressing, discovery, description, control, eventing, and presentation of devices and their encapsulated services. The major advantage of DPWS over UPnP is its strict adoption of standard WS-* specifications. This makes DPWS very attractive in industrial automation because the complexity and costs for integrating device-level processes into the

existing information technology (IT) are minimized. IEC 61850 defines a set of abstract objects and services that allows the description of functions and applications independently of a particular protocol or PHY device. The following list summarizes the overall key requirements for application-layer protocol mappings to IEC 61850 [45]:

- Standards based
- Support for utility enterprise IT and networking
- Multivendor interoperability
- Support for autoconfiguration
- Support for self-description
- Support for security
- Support for file transfers

14.5.3 Other Open-Research Issues

In the midst of a struggle to be adopted and implemented, the V2G research direction has many works that try to introduce, evaluate, confirm, and encourage its establishment. As suggested in Reference 47, the discharge of EVs affects the power grid in four different aspects: economy, battery life, providing ancillary services, and compensating intermittency of renewable energy generation. Furthermore, it is noted that charging and discharging management strategies in different case studies represent a significant point of future research directions.

In a similar context, Reference 48 enriches the research toward the optimal operation of charging stations considering the real-time electricity prices and V2G capacity. Their simulations show considerable economic and reliability benefits that need further investigation. On the same issue, the authors of Reference 49 conclude that PHEV penetration will have a great impact on the residential electricity distribution network and, as a result, the management of PHEV charge/discharge schedule is a key issue in the research of PHEVs. On the other hand, in Reference 50, the authors highlight the importance of the inefficiencies of V2G connections and suggest research directions.

Finally, on the front of software agent programming for PHEVs, the authors of Reference 51 describe their findings after simulating as well as implementing in real life an agent who considers individual driving behavior and battery-discharging costs. In a greater scale, development of the design, integration, simulation, and operation of a whole-system V2G model are provided in Reference 52. The authors explore four key areas of research: power system integration, V2G communications, system management, and power network simulation. Their V2G model aims toward the provision of a test bed capable of challenging the full range of technological difficulties that have yet to be overcome in the field of V2G technology.

Given that V2G technology has yet to receive a mass adoption, any research that adds value or offers positive insight toward that goal could significantly enable it. As a result, works toward better charging and discharging management strategies, optimal operation of charging stations, smarter V2G models, and more thorough simulation tools are important future research areas.

14.6 CONCLUSIONS

In this chapter, we presented a perspective of the requirements that need to be covered in the wireless communication scheme that can facilitate V2G integration completion. The survey focused on current work on utilizing an EV to the fullest, while keeping it interconnected to the power grid and other vehicles. An attempt was made to assess which out-of-the-box wireless technologies are compatible with V2G and what challenges and opportunities arise in newly introduced use cases. In this context, the challenges were divided into two separate groups, the technical and the macroscopic ones. Both groups pay special attention to the security issues that represent a crucial challenge in order to avoid, either economic damages to users or V2G application operators, or even worse side effects due to uncontrolled and wide-area power outages. Finally, this chapter provides additional open challenges and issues that are related to V2G and could be explored by researchers.

REFERENCES

1. W. Xiaojun, T. Wenqi, H. JingHan, H. Mei, J. Jiuchun, and H. Haiying, The application of electric vehicles as mobile distributed energy storage units in smart grid, in *Power and Energy Engineering Conference (APPEEC)*, Asia-Pacific, 2011.
2. J. Donadee and M. Ilic, Stochastic optimization of grid to vehicle frequency regulation capacity bids, *IEEE Transactions on Smart Grid,* 5(2), 1061–1069, 2014.
3. J. Pinto, V. Monteiro, H. Goncalves, B. Exposto, D. Pedrosa, C. Couto, and J. Afonso, Bidirectional battery charger with grid-to-vehicle, vehicle-to-grid and vehicle-to-home technologies, *IECON Industrial Electronics Society 39th Annual Conference of the IEEE*, Vienna, Austria, pp. 5934–5939, November 2013.
4. M. Erol-Kantarci, J. Sarker, and H. Mouftah, Communication-based plug-in hybrid electrical vehicle load management in the smart grid, *2011 IEEE Symposium on Computers and Communications (ISCC)*, Corfu, Greece, pp. 404–409, June 28–July 1, 2011.
5. J. Camp and E. Knightly, The IEEE 802.11s extended service set mesh networking standard, *IEEE Communications Magazine,* 46(8), 120–126, 2008.
6. M. Rogowsky, Tesla 90-second battery swap tech coming this year, *Forbes,* Retrieved 06-22-2013.
7. K. Murat, P. Manisa, and R. Saifur, Communication network requirements for major smart grid applications in HAN, NAN and WAN, *Elsevier Computer Networks,* 67, 74–88, 2014.
8. E. Zountouridou, G. Kiokes, N. Hatziargyriou, and N. Uzunoglu, An evaluation study of wireless access technologies for V2G communications, *Intelligent System Application to Power Systems (ISAP),* vol. 2011, *16th International Conference*, Creta, Greece, pp. 1–7, 25–28, September 2011.
9. M. Yilmaz and P. Krein, Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces, *IEEE Transactions on Power Electronics,* 28(12), 5673–5689, 2013.
10. S. Käbisch, A. Schmitt, M. Winter, and J. Heuer, Interconnections and communications of electric vehicles and smart grids, *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Maryland, USA, pp. 161–166, October 4–6, 2010.
11. W. W. W. C. (W3C), Efficient XML Interchange Working Group, [Online]. Available: http://www.w3.org/XML/EXI/. Accessed on March 1, 2014.

12. T. Markel, M. Kuss, and P. Denholm, Communication and control of electric drive vehicles supporting renewables, *Vehicle Power and Propulsion Conference, 2009. VPPC'09. IEEE*, Dearborn, Michigan, pp. 27–34, September 7–10, 2009.
13. H. Menouar, F. Filali, and M. Lenardi, A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks, *Wireless Communications, IEEE,* 13(5), 30–35, 2006.
14. L. Ning, J. Yusheng, L. Fuqiang, and W. Xinhong, A dedicated multi-channel MAC protocol design for VANET with adaptive broadcasting, *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, Syndey, Australia, pp. 1–6, April 18–21, 2010.
15. M. Booysen, S. Zeadally, and G.-J. van Rooyen, Survey of media access control protocols for vehicular ad hoc networks, *IET Communications,* 5(11), 1619–1631, 2011.
16. H. Guo, F. Yu, W.-C. Wong, V. Suhendra, and Y. D. Wu, Secure wireless communication platform for EV-to-grid research, *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, *IWCMC 2010*, Caen, France, June 28–July 2, 2010. pp. 21–25, ACM, 2010.
17. M. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, Smart electric vehicle charging: Security analysis, in *Innovative Smart Grid Technologies (ISGT)*, Washington, DC, USA, February 2013.
18. H. Liu, H. Ning, Y. Zhang, and L. Yang, Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid, *IEEE Transactions on Smart Grid,* 3(4), 1722–1733, 2012.
19. H. Chaudhry and T. Bohn, Security concerns of a plug-in vehicle, *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, USA, pp. 1–6, January 16–20, 2012.
20. M. Y.-W. Chia, S. Krishnan, and J. Zhou, Challenges and opportunities in infrastructure support for electric vehicles and smart grid in a dense urban environment—Singapore, *2012 IEEE International Electric Vehicle Conference (IEVC)*, Greenville, USA, pp. 1–6, March 4–8, 2012.
21. H. Liu, H. Ning, Y. Zhang, and M. Guizani, Battery status-aware authentication scheme for V2G networks in smart grid, *IEEE Transactions on Smart Grid,* 4(1), 99–110, 2013.
22. H.-R. Tseng, A secure and privacy-preserving communication protocol for V2G networks, *Wireless Communications and Networking Conference (WCNC)*, Paris, France, pp. 2706–2711, April 2012.
23. H. Khurana, M. Hadley, N. Lu, and D. Frincke, Smart-grid security issues, *IEEE Security and Privacy,* 8(1), 81–85, 2010.
24. H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications, *IEEE Transactions on Smart Grid,* 2(4), 707–714, 2011.
25. H.-R. Tseng, On the security of a unique batch authentication protocol for vehicle-to-grid communications, *2012 12th International Conference on ITS Telecommunications (ITST),* Taipei, Taiwan, pp. 280–283, November 2012.
26. B. Vaidya, D. Makrakis, and H. Mouftah, Security mechanism for multi-domain vehicle-to-grid infrastructure, *Global Telecommunications Conference (GLOBECOM 2011)*, Houston, Texas, pp. 1–5, December 2011.
27. V. Aravinthan, B. Karimi, V. Namboodiri, and W. Jewell, Wireless communication for smart grid applications at distribution level—Feasibility and requirements, *Power and Energy Society General Meeting, 2011 IEEE*, Detroit, Michigan, pp. 1–8, July 24–29, 2011.
28. S. Madi and H. Al-Qamzi, A survey on realistic mobility models for vehicular ad hoc networks (VANETs), *2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC)*, Evry, France, pp. 333–339, April 10–12, 2013.

29. S. Singh and S. Agrawal, VANET routing protocols: Issues and challenges, *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, Chandigarh, India, pp. 1–5, March 6–8, 2014.
30. H. Sharma, P. Agrawal, and R. Kshirsagar, Multipath reliable range node selection distance vector routing for VANET: Design approach, *Electronic Systems, Signal Processing and Computing Technologies (ICESC)*, Nagpur, India, 2014.
31. S. Uludag and N. S. K. Akkaya, A survey of routing protocols for smart grid communications, *Elsevier Computer Networks,* 56(11), 2742–2771, 2012.
32. Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. Yang, and M. Guizani, Securing vehicle-to-grid communications in the smart grid, *IEEE Wireless Communications,* 20(6), 66–73, 2013.
33. Y. Li, R. Wang, P. Wang, D. Niyato, W. Saad, and Z. Han, Resilient PHEV charging policies under price information attacks, *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, Taiwan, pp. 389–394, November 2012.
34. TeslaMotors, About Tesla Motors, December 2013. [Online]. Available: http://www.teslamotors.com/about/press/releases/tesla-dramatically-expands-supercharger-network-delivering-convenient-free-long. Accessed on June 11, 2014.
35. M. Yilmaz and P. Krein, Review of benefits and challenges of vehicle-to-grid technology, *2012 IEEE Energy Conversion Congress and Exposition (ECCE)*, Raleigh, North Carolina, pp. 3082–3089, September 15–20, 2012.
36. J. Driesen, K. Clement-Nyns, and E. Haesen, The impact of charging PHEVs on a residential distribution grid, *IEEE Transactions on Power Systems,* 25(1), 371–380, 2010.
37. K. J. Dyke, N. Schofield, and M. Barnes, The impact of transport electrification on electrical networks, *IEEE Transactions on Industrial Electronics,* 57(12), 3917–3926, 2010.
38. H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. Yang, Role-dependent privacy preservation for secure V2G networks in the smart grid, *IEEE Transactions on Information Forensics and Security,* 9, 208–220, 2014.
39. C. Liu, K. Chau, D. Wu, and S. Gao, Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies, *Proceedings of the IEEE,* vol. 101, no. 11, pp. 2409–2427, November 2013.
40. P. Siano, Demand response and smart grids—A survey, *Elsevier Renewable and Sustainable Energy Reviews,* 30, 461–478, 2014.
41. S. Hossein Imani, S. Asghari, and M. Ameli, Considering the load uncertainty for solving security constrained unit commitment problem in presence of plug-in electric vehicle, *Electrical Engineering (ICEE)*, Tehran, Iran, pp. 725–732, May 2014.
42. D. Tuttle and R. Baldick, The evolution of plug-in electric vehicle–grid interactions, *IEEE Transactions on Smart Grid,* 3(1), 500–505, 2012.
43. J. Haack, B. Akyol, N. Tenney, B. Carpenter, R. Pratt, and T. Carroll, VOLTTRON™: An agent platform for integrating electric vehicles and smart grid, *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, Las Vegas, Nevada, pp. 81–86, December 2–6, 2013.
44. B. Jansen, C. Binding, O. Sundstrom, and D. Gantenbein, Architecture and communication of an electric vehicle virtual power plant, *Smart Grid Communications (SmartGridComm)*, Gaithersburg, Maryland, pp. 149–154, October 2010.
45. J. Schmutzler, S. Groning, and C. Wietfeld, Management of distributed energy resources in IEC 61850 using web services on devices, *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, pp. 315–320, October 17–20, 2011.
46. U. F. S. UPnP Device Architecture 1.1. [Online]. Available: http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecturev1.1.pdf. Accessed on February 18, 2014.

47. H. Xiao, Y. Huimei, W. Chen, and L. Hongjun, A survey of influence of electrics vehicle charging on power grid, *IEEE 9th Conference on Industrial Electronics and Applications (ICIEA)*, Hangzhou, China, pp. 121–126, June 2014.
48. W. Tian, Y. Jiang, M. Shahidehpour, and M. Krishnamurthy, Vehicle charging stations with solar canopy: A realistic case study within a smart grid environment, *IEEE Transportation Electrification Conference and Expo (ITEC)*, Dearborn, Michigan, pp. 1–6, June 15–18, 2014.
49. R. Yu, J. Ding, W. Zhong, Y. Liu, and S. Xie, PHEV charging and discharging cooperation in V2G networks: A coalition game approach, *IEEE Internet of Things Journal,* 1(6), 578–589, 2014.
50. E. Dehaghani and S. Williamson, On the inefficiency of vehicle-to-grid (V2G) power flow: Potential barriers and possible research directions, *IEEE Transportation Electrification Conference and Expo (ITEC)*, Dearborn, Michigan, pp. 1–5, June 18–20, 2012.
51. D. Dallinger, J. Link, and M. Büttner, Smart grid agent: Plug-in electric vehicle, *IEEE Transactions on Sustainable Energy,* 5(3), 710–717, 2014.
52. J. Donoghue and A. Cruden, Whole system modelling of V2G power network control, communications and management, *Electric Vehicle Symposium and Exhibition (EVS27)*, Barcelona, Spain, pp. 1–9, November 17–20, 2013.