Smart Electric Vehicle Charging: Security Analysis

Mustafa A. Mustafa and Ning Zhang
School of Computer Science
The University of Manchester
Manchester, UK
{mustafm, nzhang}@cs.man.ac.uk

Georgios Kalogridis and Zhong Fan
Telecommunications Research Laboratory
Toshiba Research Europe Limited
Bristol, UK
{george, zhong.fan}@toshiba-trel.com

***Abstract*—This paper provides a comprehensive security analysis of the Electric Vehicle (EV) charging service in Smart Grid (SG) environment (i.e. the "smart" EV charging application). It first describes three EV charging scenarios, at home, at work and at public places. Based on these use-case scenarios, the paper presents a model for smart EV charging, consisted of application entities and interactions among them. It then illustrates potential message types communicated among these entities. Based on this model and the exchanged messages, the paper analyses security problems and potential security threats imposed on the entities, which leads to the specification of a set of security and privacy requirements. These requirements could be used to guide the future design of solutions for secure smart EV charging systems and/or a risk/impact assessment of such systems.**

***Index Terms*—Electric Vehicle (EV), Security, Smart Charging, Smart Grid (SG), Privacy**

I. Introduction

Smart Grid (SG) is envisioned to take full advantage of modern technologies in transforming the current electrical grid to one that functions more intelligently [1]. The aim is to make the electricity industry operate more efficiently and to provide electricity to society in a more secure, reliable and sustainable manner. One of the envisioned key elements of SG is the Electric Vehicle (EV). In addition to the environmental benefits (i.e. reduced greenhouse gas emissions), EVs also have the potential to bring economical benefits to the society (i.e. reduced operational costs and oil dependency) [2].

However, several studies [3], [4] have shown that letting people recharge EVs in an uncontrolled manner could have negative effects on the grid. The peak load can increase significantly requiring more generation capacity and upgrades in transmission and distribution networks. The gap between the base load and the peak load can be even larger resulting in inefficient utilization of the available generation capacity. Specifically, balancing the grid, i.e. matching the supply with the demand, will be more difficult requiring more spinning reserve. To minimize these negative effects, several studies [5]–[7] have suggested an approach of a "smart" EV charging, i.e. to charge EVs at times when it is most effective to users and to the grid (e.g. at off-peak times, at times with surplus of electricity generated by Renewable Energy Sources (RESes)).

EVs do not just consume electricity; they can also be used as Distributed Energy Resources (DERs). Using a Vehicle-to-Grid (V2G) technology [8], EVs can feed electricity back to the grid, thus making them an attractive facility for providing ancillary services (e.g. frequency regulation, spinning reserve, etc. [9]). Although providing these services would degrade an EV's battery lifetime due to increased number of charging cycles, the potential revenue generated from these services would compensate the battery degradation cost [8]. However, to be eligible, an ancillary service provider needs to offer at least a certain amount of flexible demand (e.g. 3MW in the UK [10]). As an EV typically has a limited battery capacity of 10-40kW [5] there is a need for a new entity, EV AGGregator (EVAGG) to aggregate the batteries of a number of EVs and represent their users in the electricity market, i.e. EVAGG will act as a middleman between users and grid operators.

In addition to EVAGGs, there will be other stakeholders too taking part in smart EV charging activities. These include Transmission System Operator (TSO), Distribution Network Operator (DNO), Data Communications Company (DCC) and suppliers (further details in §III). Different stakeholders have different aims and interests. For example, TSO would like to reduce peak loads and have more spare capacity; users would like to minimize their costs by recharging EVs at the cheapest possible price and by using them to provide ancillary services; suppliers would like to maximize their profit by selling more electricity at times when the price is higher; and EVAGGs would like to maximize their profit by aggregating more EVs and by actively participating in the electricity market. To maximize their respective profits, some of these stakeholders may take actions that may conflict with other entities' interests. Therefore, solutions designed to support smart EV charging should prevent or minimize the chances of any unfair play by any of the stakeholders and provide adequate protection against any threats or attacks launched by outsiders.

There are very few published papers on the smart EV charging topic [11]–[14]. These papers largely focus on how to optimize EV charging operations to minimize users' costs, to maximize users' profits by offering ancillary services, to maximize the use of electricity from RES, and to minimize the overall peak demand, etc. There has not been any prior study on security analysis of smart EV charging services. This paper

This research is supported by the Engineering and Physical Science Research Council (EPSRC) and Toshiba Research Europe Limited under Grant [EP/I1501541/1].

focuses on the latter problem. It first describes a generic model for smart EV charging drawn from the various charging use-case scenarios we have identified. It then analyses security problems of the applications using this model, before specifying a set of security requirements necessary to safeguard the operations of smart EV charging. These requirements could be used to guide a future design of a secure system to support smart EV charging and/or be used to assess risks in such a system. In detail, the rest of the paper is organized as follows: §II gives smart EV charging use-case scenarios; §III describes the generic model drawn from these scenarios; §IV analyses potential security threats/attacks in the model; §V specifies a set of security requirements, and, further discussions are given in§VI. Finally §VII concludes the paper.

II. USE-CASE SCENARIOS

The Department for Transport (DfT) in the UK has suggested three different locations where an EV may be charged [15]: at home, at work and at public places.

A. At Home

Suggesting the home charging location encourages users to recharge EVs at night. In this way, the recharging may mostly take place during off-peak times when the price of electricity is cheaper. The load caused by the recharging can be spread across the distribution network increasing the grid's reliability. To support recharging at home locations, Electric Vehicle Supply Equipment (EVSE) will need to be installed on the premises of an EV user and connected to the user's Smart Meter (SM). The electricity consumed by the EV can directly be added onto the user's household electricity bill. In addition, EVSE could also measure the electricity consumed or fed back by the EV. Thus, suppliers could offer electricity tariff plans specially designed for EVs and bill them separately. Users may also have detailed information about their EVs' charging times, durations, electricity consumptions and costs.

Of course, there may be cases where an EV is recharged on premises different from its user's home, e.g. a user (U_B) visits a friend (U_A) and recharges his EV, EV_B, at U_A's home. As EV_B can consume a considerable amount of electricity, it would be desirable for U_B to bear the cost of the electricity supplied to EV_B at U_A's home. There are two ways for U_B to make this payment: (1) U_B pays U_A directly by cash; (2) U_B pays U_A via their suppliers. The latter payment method may be more convenient and socially acceptable, as there will be no direct 'business' dealings between the two users. If both users are contracted with the same supplier, then it would not be too difficult for the supplier to simply add the expenses for recharging EV_B to the account of U_B. However, U_A and U_B may use different suppliers, S_A and S_B, respectively. In such a case (EV roaming), communication and interactions between the two suppliers are necessary.

B. At Work

Parking facilities at employees' work places may also be used for charging EVs. Usually EVs are parked for 8 hours a day at these facilities during week days. During these hours EVs can be recharged if they need to top up their batteries. They can also be discharged here offering ancillary services to the grid. To support these services, EVSEs will need to be installed at work places and connected to the grid via the SMs of the corresponding companies. Initially companies having their own fleets (e.g. rent-a-car) may invest in EVSEs. EVs can be recharged from the EVSEs and the corresponding company can pay for the consumed electricity. At later stages, companies without their own fleets may also install EVSEs.

Furthermore, a company may pass on the charging and electricity costs to its employees by charging those who use the recharging service. In such cases, the EVSEs should be able to record such information as who has used how much electricity and when. Some companies, especially those which consume large amount of electricity (e.g. manufacturers), may buy electricity in bulk directly from generators for a cheaper price than the price offered by suppliers. In such cases, if the company resells the electricity to its employees at a higher price than the price it has paid for (but for the employees, this price may still be cheaper than retail electricity price), it may get the investment for the EVSEs back. This is a win-win situation for both the company and its employees: the company makes profit by selling electricity and employees recharge their EVs at a cheaper price than the retail price.

In addition, if a company has a private parking lot large enough to accommodate a large number of EVs, and if the EVs' batteries are aggregated, then they form a single large flexible load. This load can play an important balancing role in the electricity market. The company can aggregate its employees' EVs and offer ancillary services to the grid. In return, the company may be able to offer free recharging services to its employees as long as they keep their EVs plugged into the designated lot. This is another win-win situation for both the company and its employees: the company enters a new market (balancing market) and its employees may get free electricity at work.

C. At Public Places

Other potential charging places for EVs are public places such as parking lots of supermarkets, shopping malls, rest places between cities, etc. EVSEs installed at these places are likely to be used as a top-up option. In the future, there could be a fast growing market for these top-up electricity stations (similar to the petrol stations we currently have). Owners of these stations will be responsible for providing the electricity; they will be contracted with an electricity supplier. EV users may go to these stations, recharge their EVs and pay for the service used. If these stations are designed for a fast recharge (which is likely), ancillary services to the grid are unlikely to be offered by EVs or the owners of these stations.

Some residential houses/flats or commercial premises may not have dedicated off-road parking places. In such cases, EVSEs may have to be installed on streets to offer charging facilities to people who live or work on these premises. As these EVSEs are in public places, they may be accessible to any EV and they should be able to serve many users. Currently, there are some EVSEs installed at public places in the UK [16], but their use is free as they are part of the government trials. However, in the future, the use of these EVSEs may be controlled. Whoever is in charge of such EVSEs will need to contract with an electricity supplier, purchase electricity and sell it to individual EV users.

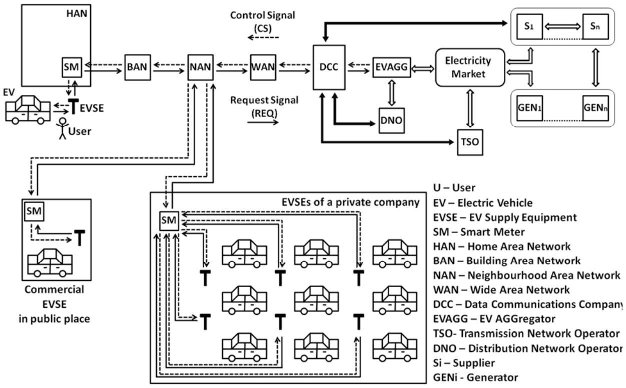

Figure 1. A generic model of a smart EV charging.

III. A Generic Model: Entities and Interactions

Based on the above use-case scenarios, we have devised a generic model for smart EV charging. This model combines the architecture proposals made by the previous studies [17]–[19], and takes into account the consultation results of the UK's smart metering implementation programme [20].

A. *Entities*

As shown in Figure 1, the model has the following entities:

- EV: a vehicle that is powered by electricity [21].
- EVSE: equipment that connects an EV to the grid [22]
- User: a person who owns an EV. The user demands, consumes and pays for the electricity used by the EV.
- SM: an advanced meter that measures electricity consumption and can perform real-time two-way communications with other entities in the SG [20].
- Networking facility: it is consisted of Home Area Networks (HANs) which are private networks located on users' premises, Building Area Networks (BANs) [23] which aggregate data from several HANs, Neighborhood Area Networks (NANs) which cover larger areas (streets) and collect data from several BANs, and, finally, Wide Area Networks (WANs) [24] which cover even larger areas (towns), collect data from several NANs and forward the data to DCC.
- DCC: an organization regulated by the UK government. It will be responsible for storing and managing data collected from SMs, and transferring the data to other authorized entities [20].
- TSO: it balances the grid using ancillary services. It also owns and manages the transmission network [25].
- DNOs: they own and manage distribution networks.
- EVAGG: it aggregates EVs, optimizes their charging processes, and provides ancillary services to TSO. In return, it offers financial incentives to EV users.
- Generator (GEN): it generates electricity [25].
- Supplier: it buys electricity from the electricity market and sells it to individual users [25].

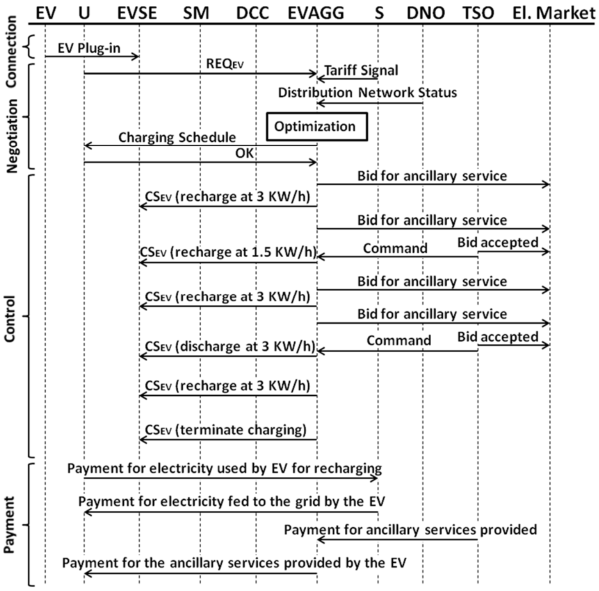
EV
U
EVSE
SM
DCC
EVAGG
S
DNO
TSO
El. Market
Connection
Negotiation
Control
Payment
EV Plug-in
REQEV
Tariff Signal
Distribution Network Status
Optimization
Charging Schedule
OK
Bid for ancillary service
CSEV (recharge at 3 KW/h)
Bid for ancillary service
CSEV (recharge at 1.5 KW/h)
Command
Bid accepted
Bid for ancillary service
CSEV (recharge at 3 KW/h)
Bid for ancillary service
CSEV (discharge at 3 KW/h)
Command
Bid accepted
CSEV (recharge at 3 KW/h)
CSEV (terminate charging)
Payment for electricity used by EV for recharging
Payment for electricity fed to the grid by the EV
Payment for ancillary services provided
Payment for the ancillary services provided by the EV

Figure 2. Interactions in a smart EV charging on private premises.

B. *Interactions among Entities and Message Types*

Potential message types and interactions among the entities in a smart EV charging activity on private premises are summarized in Figure 2. The interactions may include:

1) *Connection:* A user plugs the EV into the EVSE.

2) *Negotiation:* The user negotiates with the EVAGG.

a) User's preferences: A user sends a charging request (REQ$_{EV}$) to EVAGG. REQ$_{EV}$ may include information such as targeted State-of-Charge (SOC) at time *x* (e.g. fully recharged battery by 7am). The preferences may include information such as recharge with electricity from RES, recharge at off-peak time, offer ancillary services, etc. The user's identity will also be included in REQ$_{EV}$, so the EVAGG could incentivize the correct user for the ancillary services provided by the EV.

b) Current status: EVAGG obtains information such as the grid's status from DNOs, the electricity tariff plan at the charging location from a supplier, when and how much electricity is expected from RESes, etc.

c) Optimization: EVAGG analyses the data, works out an optimal charging schedule for the EV (in accordance with the user's preferences), and sends the schedule to the user.

d) Confirmation: The user may accept the schedule, ask for rescheduling or reject it and start an uncontrolled recharge.

3) *Control:* EVAGG manages the EV's charging process in accordance with the agreed schedule by sending control signals (CS$_{EV}$) to the EVSE. It also constantly bids at the electricity market to offer ancillary services. If its bid is accepted, it will receive a command to change its overall demand. To comply with the command, the EVAGG may change the EV's charging shedule. In spite of these changes, the targeted SOC should be reached by the end of the session.

4) *Payment:* There may be three possible payment flows related to the user.

- The user pays the supplier for the electricity consumed by the EV.
- The user receives payments from the supplier for the electricity discharged from the EV and fed to the grid.
- The user receives payments from the EVAGG for any ancillary services offered by the EV to the grid.

IV. Threat Analysis

While smart EV charging has a potential to bring financial benefits to various entities, it may also offer opportunities for some entities to take advantage of the others in order to maximize their benefits. This section analyses how various entities in the model may cheat or commit security breaches.

A. Impersonation

Impersonation is the theft of another entity's identity. In the smart EV charging application some entities may try to launch such attacks. For example, a dishonest user may try to impersonate another user in an attempt to recharge an EV for free (by plugging the EV into a socket connected to the SM of the victim) or to receive any incentives for ancillary services offered by the victim's EV (by intercepting and manipulating REQEV sent by the victim); a dishonest supplier may try to impersonate an EVAGG in an attempt to increase its sales at peak times or an external attacker may try to impersonate the EVAGG in an attempt to take control of the charging process (by forging legitimate CSEV). The aims of these attacks could be to seek financial gains, to cause disruptions in the charging processes or to just cause nuisance.

B. Tampering with Communication Messages

Fraud or harm may also be committed by tampering with the messages sent among the participating entities (e.g. REQEV, CSEV, etc.). Tampering may be done by using one of the following ways: modifying, delaying or replaying a legitimate message, or inserting illegitimate messages into the underlying network. Tampering with legitimate messages can cause damages to the grid's stability and/or inconveniencies to users. For example, if an adversary modifies CSEV content from "*recharge*" into "*discharge*", the user will find his EV with a fully discharged battery. This may force the user to recharge the EV at a peak time. In such case, the user will not only suffer from inconvenience, but also some financial losses. A similar situation may arise if a CSEV, assigned to a specific EV, is modified to control another EV. Delaying important CSEV messages could affect the grid's stability and cause brownouts. Replay attacks may also cause damages. For example, if an adversary captures a REQEV "*start recharge*" message sent at an off-peak time, but replays it at a peak time, the user will have to pay a higher price for the electricity. Injecting fake messages into the network could cause congestion, which may delay successful deliveries of other legitimate messages causing service delays or disruptions.

C. Eavesdropping

REQEV and CSEV may contain sensitive information about an EV and its user (e.g. identities, account details, etc). If an adversary can read these personal details, he may be able to impersonate the user or user's EV. In addition, REQEV and CSEV may contain information that has commercial values to other parties. For example, battery manufacturers may be interested in knowing how frequently EV batteries are recharged. With access to such information, the battery manufacturers may be able to identify the most used EVs and market their products to the users of these EVs.

D. Denial-of-Service

One of the objectives in controlling an EV charging process is to reduce the chances of putting the grid in an imbalance state. Ensuring reliable and on-time delivery of communication messages and reliable operations of EVAGG is essential to achieve this objective. DoS attacks on channels and services may delay message deliveries and make services inaccessible to legitimate users. One example of such attacks is tampering with pricing signals sent to users (i.e. modifying the price to a very low level). This attack could result in a large number of REQEV signals being sent to the EVAGG almost at the same time. A potential consequence of these DoS attacks is an unstable grid or even blackouts.

E. Privacy Breaches

Security problems may also be caused by authorized insiders. Privacy breaches are an example of such problems. Legitimate entities may use the opportunities to build users' profiles for purposes that are not directly relevant to smart EV charging. For example, an EVAGG may gather information about EVs and their charging locations. Using this information the EVAGG may build a profile of a user. EVAGG may even sell this information to other interested parties.

F. Disputes

As the EV charging process has financial implications to all the entities involved, there are incentives for any of the entities to fraudulently try to obtain some financial gains or to reduce their costs. For example, EVAGG may try to control an EV without having its user's permission. Similarly, if a user sends a REQEV "*recharge **now***" instead of "*recharge **when the price is below x***" by mistake, the user may later deny having sent the REQEV and blame the EVAGG for the high recharging costs. Such dishonest and/or accidental actions may lead to disputes between different entities. Having to deal with such disputes may put off users from participating in smart EV charging programs. Therefore, for the success of these programs necessary technical measures should be in place to ensure that any potential disputes between the entities can be resolved promptly and fairly.

V. Security Requirements

Based on the above threat analysis, this section specifies a set of security requirements for a smart EV charging service. Figure 3 illustrates some proposed actions or security services to counter the threats/attacks identified in the previous section.

A. Entity Authentication

Entity authentication assures that a communicating entity is the one that it claims to be. To counter impersonation attacks and to provide a fair billing with an EV roaming support, strong entity identification and mutual authentication services should be provided. These include authentication between:

- EV*i* and UA – ensures that only EVs authorized by UA can connect to the grid via EVSEA.
- UB and SB – ensures that the electricity used by the EVB is accounted to its user, UB.
- EVB and SB – ensures that UB is accounted only for the electricity used by the EVB.
- UB and EVAGGB – ensures that any incentives for the ancillary services offered by EVB are accounted to UB.

B. Message Authenticity

Message authenticity assures that messages (e.g. REQEV, CSEV, payments, etc.) are exactly what have been sent by the claimed entities. To counter tampering attacks the authenticity of these messages should be provided. Keyed *hash* values, *Message Authentication Code*, or *digitally signed tokens* (through the use of public key cryptography) [26] are typically used to counter these attacks and to ensure the messages' integrity. Usually, in such a cryptographically protected token, a *nonce* (a random arbitrary number used only once) or a *time stamp* is enclosed to ensure that replay attacks can be detected.

C. Authorisation

Authorization is the process of granting authorized users legitimate access to resources (systems, data, applications, etc). To minimize the chances of successful impersonation attacks, UA should always authorize EVs requesting to use EVSEA for the first time. Furthermore, all metering or usage related data are expected to be managed by the DCC. To prevent misuse of the data, the DCC should impose access control of data based on the principle of least privilege, e.g. only grant EVAGGB the access to data related to the charging of EVB. An access control mechanism, e.g. *Role Based Access Control* (RBAC), may be exploited to serve this purpose.

D. Confidentiality

Confidentiality is a protection of data from any unauthorized disclosure. To counter eavesdropping attacks the confidentiality of REQEV, CSEV, payments, etc. should be protected. Confidentiality of these messages can be provided by using an encryption technique such as *symmetric encryption, public key encryption* or a combination of both.

E. Non-repudiation

Non-repudiation (NR) provides protection against false denial of having participated in a communication/transaction. There are two aspects of NR: NR of Origin (NRO) and NR of Receipt (NRR). NRO provides protection against a sender's false denial of having sent a message. NRR provides protection against a receiver's false denial of having received a message. In smart EV charging scenarios the following NR requirements should be considered:

- NRO of REQEV - EVAGGB holds evidence that UB has sent a REQEV.
- NRR of REQEV - UB holds evidence that EVAGGB has received the REQEV.
- NRO of CSEV - EVB holds evidence that EVAGGB has sent a CSEV.

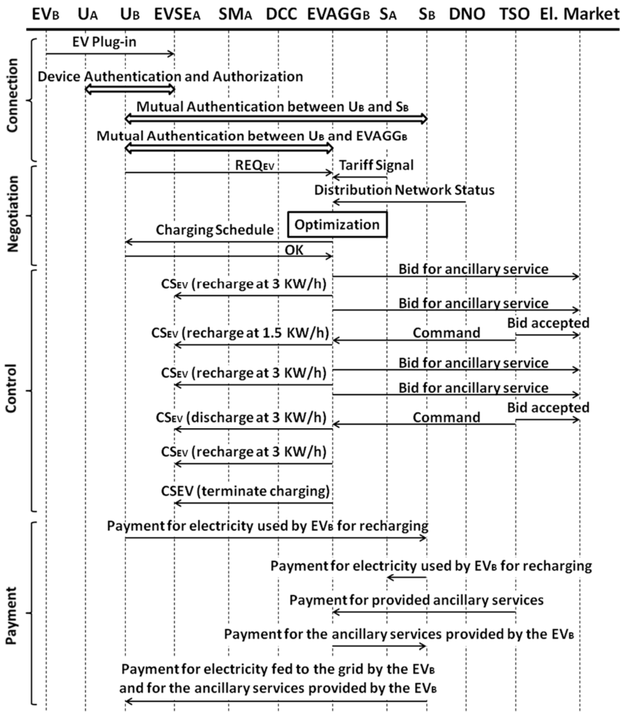
EVB
UA
UB
EVSEA
SMA
DCC
EVAGGB
SA
SB
DNO
TSO
El. Market
Connection
EV Plug-in
Device Authentication and Authorization
Mutual Authentication between UB and SB
Mutual Authentication between UB and EVAGGB
Negotiation
REQEV
Tariff Signal
Distribution Network Status
Optimization
Charging Schedule
OK
Control
Bid for ancillary service
CSEV (recharge at 3 KW/h)
Bid for ancillary service
Bid accepted
CSEV (recharge at 1.5 KW/h)
Command
Bid for ancillary service
CSEV (recharge at 3 KW/h)
Bid for ancillary service
Bid accepted
CSEV (discharge at 3 KW/h)
Command
CSEV (recharge at 3 KW/h)
CSEV (terminate charging)
Payment
Payment for electricity used by EVB for recharging
Payment for electricity used by EVB for recharging
Payment for provided ancillary services
Payment for the ancillary services provided by the EVB
Payment for electricity fed to the grid by the EVB
and for the ancillary services provided by the EVB

Figure 3. A smart EV charging application that supports users' mobility in accessing electricity and in making payments.

- NRR of CSEV - EVAGGB holds evidence that EVB has received the CSEV.

To enhance the level of trust between UB and EVAGGB, all the actions taken by them should be unforgeable, undeniable and traceable. This is necessary to ensure a fair resolution of any dispute. A number of cryptographic building blocks, including *digital signatures*, *recoverable* and *verifiable tokens* [26] and *off-line trusted third parties* (TTPs) may be used to provide the NR properties.

F. Availability

Availability is the property of a system or a system resource being accessible and usable upon demand by authorized system entities. DoS attacks impose a threat to this property. Measures must be in place to ensure that important service entities (e.g. DCC, EVAGGB) can resist DoS attacks.

G. Anonymity and Non-linkability

Anonymity is a property of not being identifiable within a set. In our problem context, anonymity may be used to prevent UB's real identity from being revealed to EVAGGB during a charging process, and/or prevent UB's charging location from being linked to UB's real identity. Non-linkability protects EVB's multiple charging sessions from being linked together and protects UB's multiple charging sessions from being linked to UB's real identity. To preserve UB's privacy, both anonymity and non-linkability properties should be provided. This can be achieved by assigning a dynamic identifier to each of the charging sessions performed by UB. Of course, a controlled and authorized linkage of UB's multiple charging sessions should be supported, as this is necessary to ensure accountability and traceability in the event of a dispute or security incident. As SB has to know the real identities of UB and EVB (for authentication and billing purposes), it may be a candidate TTP and this TTP may be the only entity which knows the connection between UB's real and dynamic identity. In more general cases, EV charging anonymity may be provided via a secure escrow service [27].

VI. Further Discussions

A smart charging of the roaming EVB on the premises of UA and payment for using this service involve the participation and interactions of multiple entities such as UA, UB, EVSEA, SMA, DCC, SA, SB, EVAGGB, DNO, TSO and DCC. These also generate different data items intended for different users (entities) and with varying levels of sensitivity. The different entities should therefore have different access privileges in accessing these data items. Any unauthorized access of the service and/or data generated by the service, or any malicious, selfish or dishonest attempt, by any of the entities could potentially harm the interest of other entities. In addition, different households often register with different suppliers (regardless of their physical location), some households may change suppliers from time to time (to hunt for better deals), each household may have multiple EVs registered with different occupants of the household, and some entities (e.g. SMA, EVSEA) may have limited computational capabilities. All these issues and characteristics dictate that existing security solutions, such as virtual private networks and secure socket layer (SSL), are not readily applicable to the smart EV charging application. More work is necessary to investigate and design security solutions that at the same time satisfy the requirements specified in §V and accommodate the aforementioned issues and characteristics of the application.

The importance of securing the emerging SG is well recognized by standardization organizations such as NIST [17], IETF [28] and international communities, e.g. ETSI [29]. As EVs will be a major player in the SG, the security of EV related applications should also be addressed. Conducting the security analysis is the first step towards this direction. The requirements discussed in §V may serve as a benchmark for designing and evaluating future secure solutions to support smart EV charging. They may also be used for devising a risk model for quantitative analyses of risks and costs incurred to the various stakeholders in the EV charging system.

VII. Conclusion

Although EVs can provide a number of environmental and financial benefits, their uncontrolled charging can destabilize the grid. This can be prevented by employing "smart" EV charging. However, this new paradigm can bring a wide range of security issues. In this paper, we have devised a model of smart EV charging and analyzed security problems and potential security threats using this model. Based on this security analysis we have specified a set of security requirements, which will be used to guide the next stage of our work (i.e. the design of a reliable and secure payment service that supports EV roaming on private premises) towards the design of a secure smart EV charging system.

References

[1] H. Farhangi. The path of the smart grid. *Power and Energy Magazine, IEEE*, 8(1):18–28, Jan.-Feb. 2010.

[2] Investigation into the scope for the transport sector to switch to electric vehicles and plugin hybrid vehicles. Technical report, BERR & DfT, Oct. 2008.

[3] J. Driesen *et al*. The impact of vehicle-to-grid on the distribution grid. *Electric Power Systems Research*, 81(1):185– 192, 2011.

[4] K.J. Dyke *et al*. The impact of transport electrification on electrical networks. *Industrial Electronics, IEEE Trans*,57(12):3917–3926, 2010.

[5] Wencong Su, H. Eichi, Wente Zeng, and Mo-Yuen Chow. A survey on the electrification of transportation in a smart grid environment. *Industrial Informatics, IEEE Transactions*, 8(1):1–10, Feb. 2012.

[6] F. Geth *et al*. Impact-analysis of the charging of plug-in hybrid vehicles on the production park in belgium. In *MELECON 2010 - 15th IEEE Mediterranean Electrotechnical Conf.*, pages 425–430, Apr. 2010.

[7] A. Brooks, E. Lu, D. Reicher, C. Spirakis, and B. Weihl. Demand dispatch. *Power and Energy Magazine*, IEEE, 8(3):20–29, May, 2010.

[8] Willett Kempton and Jasna Tomić. Vehicle-to-grid power fundamentals: Calculating capacity and net revenue. *Journal of Power Sources*, 144(1):268–279, Jun. 2005.

[9] Tu Yiyun, Li Can, Cheng Lin, and Le Lin. Research on vehicle-to-grid technology. In *Computer Distributed Control and Intelligent Environmental Monitoring, 2011 Int. Conf.*, p 1013– 1016, Feb. 2011.

[10] National grid. Internet: www.nationalgrid.com/uk [24.04.2012].

[11] L. P. Fernández *et al*. Assessment of the impact of plug-in electric vehicles on distribution networks. *Power Systems, IEEE Transactions*, 26(1):206–213, Feb. 2011.

[12] Y. Cao *et al*.An optimized ev charging model considering tou price and soc curve. *Smart Grid, IEEE Transactions*, 3(1):388–393, Mar. 2012.

[13] S. Deilami *et al*. Realtime coordination of plug-in electric vehicle charging in smart grids to minimize power losses and improve voltage profile. *Smart Grid, IEEE Transactions*, 2(3):456–467, Sept. 2011.

[14] O. Sundstrom and C. Binding. Flexible charging optimization for electric vehicles considering distribution grid constraints. *Smart Grid, IEEE Transactions*, 3(1):26–37, Mar. 2012.

[15] Making the connection the plug-in vehicle infrastructure strategy. Technical report, Department for Transport, June 2011.

[16] Ev network uk. Internet: www.ev-network.org.uk/ [24.04.2012].

[17] U.S. NIST, Guidelines for smart grid cyber security (vol. 1 to 3), NIST IR-7628, Aug. 2010.

[18] F. Marra, *et al*. Electric vehicle requirements for operation in smart grids. In *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES Int. Conf. and Expo*, pages 1–7, Dec. 2011.

[19] J.M. Jorgensen, S.H. Sorensen, K. Behnke, and P.B. Eriksen. Ecogrid eu - a prototype for european smart grids. In *Power and Energy Society General Meeting, 2011 IEEE*, pages 1–7, Jul. 2011.

[20] Smart metering implementation programme: A consultation on the detailed policy design of the regulatory and commercial framework for dcc. Technical report, DECC, 29 Sept. 2011.

[21] C.C. Chan. The state of the art of electric, hybrid, and fuel cell vehicles. *Proc. IEEE*, 95(4):704–718, Apr. 2007.

[22] A.M. Foley *et al.* State-of-the-art in electric vehicle charging infrastructure. In *Vehicle Power and Propulsion Conf. (VPPC), 2010 IEEE*, pages 1–6, Sept. 2010.

[23] Z.M. Fadlullah, M.M. Fouda, N. Kato, Xuemin Shen, and Y. Nozaki. An early warning system against malicious activities for smart grid communications. *Network, IEEE*, 25(5):50–55, Sept.-Oct. 2011.

[24] Yilin Mo *et al*., Cyberphysical security of a smart grid infrastructure. *Proc. IEEE*, 100(1):195–209, Jan. 2012.

[25] The electricity trading arrangements: A beginners guide. Technical report, Elexon, Jul. 2009.

[26] William Stallings. *Cryptography and Network Security Principles and Practices.* Prentice Hall, 4th edition, 2005.

[27] C. Efthymiou and G. Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGrid-Comm), 2010 First IEEE Int. Conf.*, pages 238–243, USA, Oct. 2010.

[28] IETF RFC 6272: Internet Protocols for the Smart Grid Internet: www.tools.ietf.org/html/draft-baker-ietf-core [24.04.2012].

[29] ETSI. Machine-to-machine communications (m2m); threat analysis and counter-measures to m2m service layer. Technical report, ETSI TR 103 167 V1.1.1, Aug. 2011.