Efficient Certificate Verification for Vehicle-to-Grid Communications

Nico Saputro[1], Samet Tonyali[1], Kemal Akkaya[1], Mumin Cebe[1], and Mohamed Mahmoud[2]

[1] Department of Electrical & Computer Engineering, Florida International University, Miami, FL 33174 USA
Email: {nsapu002, stonyali, kakkaya, mcebe}@fiu.edu
[2] Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN, 38505 USA
Email: mmahmoud@tntech.edu

Abstract. While public charging stations are typically used for Electric Vehicle (EV) such as charging, home microgrids that may act as private charging stations are also expected to be used for meeting the increased EV charging demands in the future. Such home microgrids can be accessible through their smart meters, which makes advanced metering infrastructure (AMI) a viable alternative for vehicle-to-grid (V2G) communications. However, to ensure secure V2G communications using public-keys, smart meters will need to maintain certificate revocation lists (CRLs) not just for the AMI network but also for large number of EVs that may interact with them. For resource-constrained smart meters, this will increase the storage requirements and introduce additional overhead in terms of delay and CRL maintenance. To eliminate this burden, we propose keeping merely non-revoked certificates that belong to EVs, which are usually driven within the vicinity of that particular microgrid. The motivation comes from the fact that it is inefficient to distribute and store a large CRL that has revocation information about all EVs in the whole system as most of these EVs will never come to the geographic vicinity of that home microgrid. The approach ensures that any status changes of these certificates are communicated to the smart meters. We implemented the proposed approach in a realistic V2G communication scenario by using IEEE 802.11s mesh as the underlying AMI infrastructure using ns-3 simulator. The results confirmed that the proposed approach significantly reduces the certificate verification time and the storage requirements on smart meters.

1 Introduction

Electric Vehicles (EVs) have recently received increasing popularity to reduce carbon dioxide emissions and promote adoption of intermittent renewable energy sources by acting as energy storage systems [1]. Although EVs currently constitute a narrow segment in the market, mass penetration and market dominance are expected in the upcoming years in the US, particularly with reduced

production costs, such as for Tesla's new Model 3 which has already globally garnered 400K pre-orders. Currently, more than 15,000 public charging stations and 42,000 charging outlets have already been deployed in the US [2] for charging EVs. However, due to various constraints such as investment costs and proximity to grid services, public stations may not be able to address the growing charging needs. Such a need is expected to be met by exploiting the existing microgrid users (i.e., homes/campuses that can generate energy via solar or wind) who are willing to sell their excess power to the grid or EV users. In particular home microgrids (often dubbed a nanogrid) are on the rise with the innovations in the current power grid systems [3]. In this way, EV users will have abundant options to charge their vehicles by communicating with the microgrid/nanogrid owners that will act as residential charging stations.

However, the use of microgrids for EV charging requires a communication infrastructure to connect EVs with the microgrids in certain neighborhoods. Besides the option of building a new and completely separate V2G communication infrastructure between microgrids and EVs, utilizing the existing infrastructures can be an option due to reduced costs. Therefore, we advocate use of existing AMI that connects home microgrids to each other and to power grid via wireless communications. Specifically, a smart meter in a home can act as the connection point to communicate with the EVs and utility/third parties. However, one needs to ensure the security of these communications. For instance, once a malicious EV is connected to the Smart Grid infrastructure via AMI, it can perform denial of service attacks or inject false data to the grid.

An integral part of a security solution for V2G is a dedicated public key infrastructure (PKI), which ensures security issues such as confidentiality, authentication, integrity, etc. In our case, this also raises new challenges related to the operation of such a PKI. First of all, there are different energy providers (utility companies) in a country or state. They may all have different PKIs for providing these services to their customers. However, the EVs would travel to different places and thus will need to charge from a station that is served by another utility company. This will necessitate cross-certification among different utility companies.

Second, as there would be a large number of vehicles in a state, the size of the certificate revocation list (CRL), which keeps the revoked certificates, is expected to be significantly large. From the perspective of smart meters, in addition to the management of public key certificates for AMI network, communications with EVs would require adding a new CRL specific to vehicles, which will significantly increase the space requirements for smart meters. Moreover, frequently updating and distributing CRLs to a large number of smart meters is a big burden, while few vehicles may make a connection with that smart meter.

Finally, verifying signatures from fast moving EVs will be a challenge in terms of latency requirements. This is because, the EV must finish message exchanges before leaving the wireless coverage area of the smart meter. As a consequence, if a large portion of this time is spent with certificate verification, then there might not be enough time left to complete message exchanges among

two parties successfully. In addition to that, mobile nature of communication makes reliable transmission even more challenging.

Considering these issues, in this paper we tackle the problem of CRL management for V2G communications in multi-provider environments. We first present an architectural model for PKI and secure V2G communications. Then, we propose an efficient mechanism to reduce the storage requirements for CRL management while still providing a reduced communication delay for EV-smart meter message exchanges. Our mechanism is based on the idea of keeping the certificates of EVs of interest in the smart meters rather than following the traditional way of dealing with CRLs.

The idea stems from the fact that EVs in a certain area typically do charging at nearby microgrids. The number of foreign EVs (the EVs that are coming out of town or state) is far less than the number of domestic EVs (the EVs that are coming from the town). Therefore, there is no need to maintain their revoked certificates in the CRLs. Rather, we keep an up-to-date local list of frequently used and *valid* certificates so that EVs in the neighborhood will quickly get verified by checking this *local list* in the smart meter. If a certificate is not in the list, a smart meter can connect to the utility company that has access to up-to-date CRL for every EVs and smart meters. In other words, our proposed approach asks the certificate authority only when a new certificate is presented to a smart meter rather than asking all the time as in the case of traditional approaches [4]. Note that any new revocations for the valid certificates in the local list will be sent to the smart meters by the utility company so that they can be removed.

To assess the performance of the proposed mechanism, we conducted simulations in ns-3 network simulator by implementing an IEEE 802.11s-based wireless mesh network among the smart meters and integrating it with EVs acting as clients. EV-smart meter communication was assumed to be based on Dedicated Short Range Communications (DSRC) [5], which is the current vehicular communication standard for safety applications. The experiments looked at various cases to investigate the gains through using a local valid certificate list. The results indicated that the size of such a list is smaller compared to traditional CRLs and that signature verifications can be achieved with higher success rates in small communication delays compared to Online Certificate Status Protocol (OCSP) [6] which is the current standard used on Internet.

This paper is organized as follows. In the next section, we describe the related work. Section III is dedicated to the proposed system model and PKI. In Section IV, we explain our proposed approach for certificate revocation in details. Section V provides the results of experimentation and Section VI concludes the paper.

2 Related Work

A number of approaches have been proposed to provide secure V2G communications. Some of these studies dealt with certificate issues. For instance, Falk and Fries [7] studied possible attacks stemming from V2G integration and presented

the requirements in order to avoid and mitigate from attacks. It is recommended to use short term certificates and OCSP [6] in order to make sure that a certificate is still valid. This requires frequent access to CA servers which may not be feasible. In this regard, another option could be to use OCSP *stapling* [8] where the EVs query the OCSP server at certain intervals and obtain a signed timestamped OCSP response. When any of the EVs attempt to connect to the grid, this response which is directly signed by the certificate authority is included ("stapled") in the certificate. Again, this approach also requires the EVs to connect the certificate authority frequently. Moreover, in order to ensure the signed timestamped OCSP response in the EV's certificate is legitimate, a smart meter must have the public key of the certificate authority who signs the OCSP response. In another approach, Zhang et al. [9] introduced a context-aware authentication scheme for V2G systems based on battery status of the EV. Rather than using a PKI, the EV computes its authentication operators based on an access challenge sent by the local aggregator. However, the authentication of an EV moving from one network to another is presented as an open issue. Our work differs from the aforementioned approaches by considering the case of EV to AMI communication through smart meters and introducing the idea of maintaining valid certificates. In addition, our approach does not require EVs to frequently access their CA.

In addition to security issues for V2G communications, a number of other studies looked at the design of a PKI for this type of communication. For instance, Vaidya et al. [10] proposed a hybrid PKI involving hierarchical and peer-to-peer cross-certification. In the proposed PKI model, intra-domain and inter-domain certification management techniques use Elliptic Curve Qu-Vanstone as implicit certificates since they do not require explicit verification of the certificate authority signature, so they are smaller in size resulting in using the bandwidth efficiently. Later, they discussed the issue of inter-domain PKI trust and proposed another solution based on a peer-to-peer elliptic curve cryptography-based cross-certification mechanism and a self-certified public key technique [11]. In addition, they proposed a certificate path processing technique for the proposed PKI model. Baumeister and Dong [12] suggested the use of Bridged trust model and a compromise of OCSP and CRL model as the ideal models for the V2G system. Finally, Multin and Schmek [13] introduces the project Hubject that enables charging an EV at energy providers other than the one with which the EV has signed a contract. These energy providers should be connected to a clearing house so that the certificates from different providers can be in an interplay for an authenticated communication. In this paper, we utilize a PKI model similar to the Bridge model in [12] and allow participating energy providers to charge EVs in different providers.

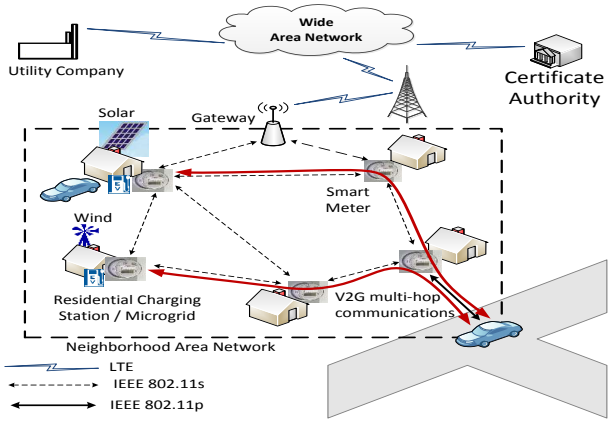


Fig. 1: Vehicle-to-Grid Infrastructure. An EV can communicate with multiple microgrids through smart meters to request some information or to make a charging reservation while the EV is still on the road through V2G multi-hop communications.

3 Vehicle-to-Grid Model

3.1 Model Description

Since our goal is to utilize the existing infrastructure, we consider the available communications options in both vehicular and smart grid for V2G model. Currently, while there is already DSRC standard [5], which is based on IEEE 802.11p, for vehicle-to-vehicle (V2V) communications, there are a variety of options for multi-tier Smart Grid communications networks [14]. Wireless mesh is one of the viable options and widely adopted for smart meter communications by major AMI vendors [15]. Between these two options, we use IEEE 802.11p instead of IEEE 802.11s [16] for the communication between EV and smart meter since our proposed approach requires a reliable and low communication latency in highly mobile environment. IEEE 802.11p was designed for such environments.

Fig. 1 represents the considered V2G model for a utility company. A number of residential wireless-enabled smart meters in an area forms an AMI neighborhood area network. This AMI uses a gateway to connect to the utility company through a wide area network. Each smart meter operates as a dual-interface node with the functionality of IEEE 802.11s multi-hop wireless mesh network for AMI application and IEEE 802.11p for communication with an EV.

The gateway also operates as dual-interface node with the functionality of IEEE 802.11s and Long Term Evolution (LTE). It acts as the IEEE 802.11s root node as well as the portal node to the utility company through LTE network [17] [18]. A GPS-enabled On-Board Unit with an IEEE 802.11p interface is available on every EV to support vehicle-to-grid, vehicle-to-vehicle, and vehicle-to-infrastructure communications.

In our scenario, due to the availability of multiple options of residential charging stations in an area, an EV can collect the residential charging station information (e.g., cost, availability, distance, and time required for charging), select

the residential charging station, and make a reservation to a residential charging station while the EV is still on the road through the proposed V2G model. Since security is paramount importance for Smart Grid, an EV must first authenticate itself using PKI to the nearest smart meter of the AMI network using IEEE 802.11p before it can use the multi-hop capability of IEEE 802.11s to reach the intended residential charging station(s) for querying or charging reservation. In this way, an EV_i can reduce its traveling time without consuming its battery too much for finding the closest residential charging station that meets its criteria. The considered model also supports out-network/roaming/inter-provider charging where EV_k from a utility company UC_p can use other utility companies' charging stations while the charging usage still be billed to the EV_k account in UC_p through the third party such as a clearing house.

3.2 Problem Motivation and Definition

In our scenario, digital certificates are used to verify the sender's identity in V2G communication. However, it is necessary to identify and remove revoked certificates to prevent misbehavior or attacks. One of the different approaches that are used for this purpose is CRLs. This is a commonly used method in traditional PKIs. However, this approach has some drawbacks when applied to our setting. First, the CRL size can become huge considering the large number of EVs. In particular, since the vehicles are expected to change their identities frequently due to privacy requirements [5], the size will be even larger. Second, the CRL needs to be distributed to every smart meter in a timely manner. However, increased CRL size will create a distribution as well as storage problem if there are not enough resources on the device. This is the case for smart meters. In fact, a smart meter already has a different CRL for AMI communications [19] [20]. A second CRL for EVs would definitely be a storage and maintenance burden. As discussed in [21], even distributing a small file such as firmware updates to all smart meters in an AMI network requires a significant amount of time. Yet, EVs will have limited time to communicate with a smart meter due to their mobility. Thus, it would be better to have a locally available CRL on the smart meter to speed up the verification process.

In this paper, we tackle this problem of certificate revocation management for V2G communications. Specifically, our goal is to come up with an efficient mechanism to not only reduce storage requirements but also consider the latency constraints in V2G communications.

4 An Efficient Certificate Verification Scheme

4.1 Motivation and Approach Overview

Our main challenge is to be able to quickly verify the certificate of any EV on the road that is trying to communicate with the smart meter of potential residential charging station for charging information (e.g., the available charging

time and duration, charging capacity, etc) since the contact time for an EV with a smart meter might not be that long due to speed of the EV. Obviously, the traditional solution is to always maintain an up-to-date CRL on the smart meter of residential charging station (i.e., distributed CRL (D-CRL) scheme) so that a quick local search can be conducted on the smart meter. However, this solution would bring a huge overhead on the smart meter in terms of space and communications. The size of this CRL would be very large due to the large number of EVs and this CRL needs to be updated frequently even though the smart meter never uses it. This is particularly a problem when the location is considered. Typically, a certain residential charging station/microgrid will serve the needs of EVs in the neighborhood or town. There will be rarely foreign EVs that would like to charge there (e.g., roaming charging). Thus, for such rare cases, the smart meter needs to maintain the CRL for all vehicles in the state/country which is an overkill.

An alternative solution would be to use OCSP, and each time the smart meter needs to verify a certificate it queries the certificate from CA so that it will not need to deal with huge size CRLs. However, in that case, it requires a communications infrastructure between every smart meter in AMI network and multiple CAs, which is not feasible. Moreover, since security is paramount importance for Smart Grid, enabling every smart meter to have direct access to multiple CAs may introduce a huge amount of new attack venue. Thus, it requires a security handling mechanisms, which eventually cause the verification of the certificate may take a long time and depending on the speed of the EV, the response may not come back on time for completing the scheduling process.

In this paper, as opposed to traditional solutions which follow a CRL-based approach, we follow a different idea to solve this problem and propose keeping valid certificates on the smart meter to speed up the process and favor the local communication requests from EVs. Specifically, whoever makes a connection with a particular smart meter will have its certificate stored on that smart meter in a list after this certificate has been verified by the utility company. This list will then be used for future communications from the same EVs. If a valid certificate is revoked in the future, the utility company should advise the smart meters that store the certificate to remove it from their list. In this way, the CRLs for foreign EVs that would never communicate with that particular smart meter again will not be maintained. The local list of valid certificates will be updated accordingly. Next, we describe the details of our valid certificates management scheme.

4.2 Certificate Verification based on Verified Certificate List

We introduce two lists for our scheme: (1) Verified Certificate List (VCL) and (2) Location-based Certificate List (LCL). A VCL is maintained in every smart meter to store a customized EV_i certificate, a partial content of the full EV_i certificate that has been verified as a valid certificate by the utility company. The minimum certificate information in the customized EV_i certificate are EV_i identity, EV_i certificate serial number, EV_i public key, certificate authority issuer

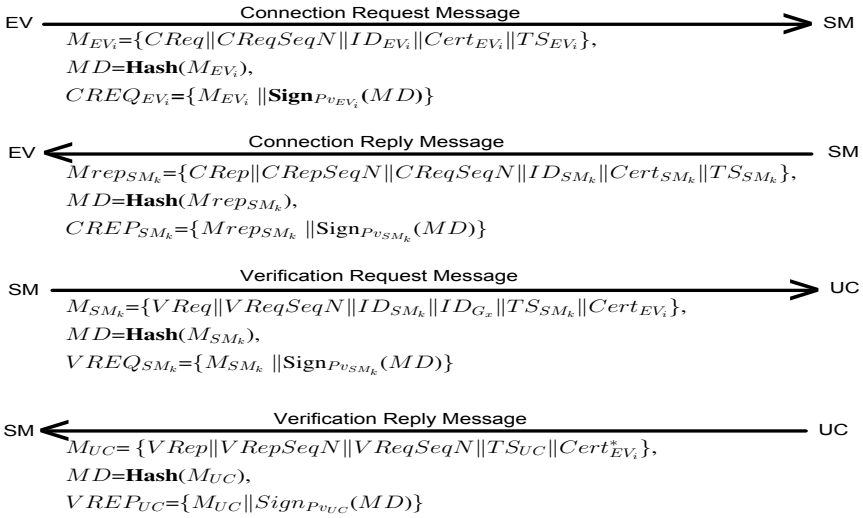


Fig. 2: Message Exchanges

Table 1: Notations

Acronym	**Description**
SM, EV, UC, CA, G, ID, TS, MD	Smart meter, Electric vehicle, Utility company, Certificate authority, Gateway, Identity, Timestamp, message digest
$CReq$ & $CReqSeqN$	connection request id & sequence number
$CRep$ & $CRepSeqN$	connection reply id & sequence number
$VReq$ & $VReqSeqN$	verification request id & sequence number
$VRep$ & $VRepSeqN$	verification reply id & sequence number
$Cert$ & $Cert^*$	full and customized certificate
Pub & Pub^*	unverified and verified public key
Pv,**Hash**,**Sign**	private key, hash function, digital signature

identity, and expiration date. For each customized certificate in the VCL, a *frequency attribute* is used to indicate how many times this certificate is used in this smart meter within a time interval T. LCL is maintained by the utility company and stores the list of all AMI networks' gateways. Each entry of the LCL consists of the ID of the gateway of an AMI network, the ID of a smart meter that acts as a microgrid under that gateway, and the list of all valid EV certificates (serial number and certificate authority identity) that are currently stored in the VCL of that smart meter. The notation definitions are presented in Table 1.

Before an EV_i makes a connection with a microgrid (i.e., smart meter representing it), it collects broadcast messages from the smart meters in the vicinity. The one with the strongest signal strength (i.e., SM_k) will be chosen. Then, four messages exchange for EV certificate verification and connection establishment between the EV_i and the selected SM_k are conducted as depicted in Fig. 2: (1) a connection request message $CREQ_{EV_i}$ from EV_i to SM_k; (2) a connection reply message $CREP_{SM_k}$ from SM_k to EV_i; (3) a verification request message

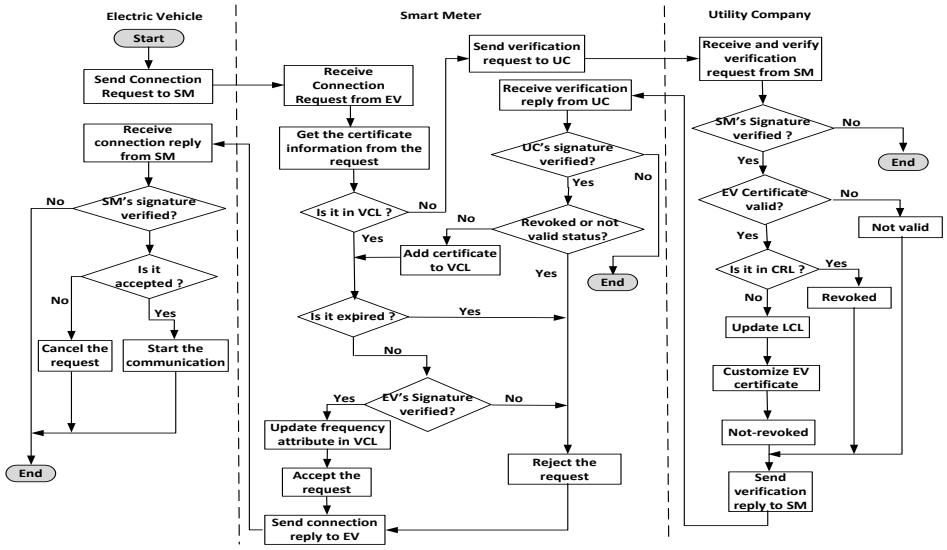


Fig. 3: Certificate Verification Process

$VREQ_{SM_k}$ from SM_k to UC; and (4) a verification reply message $VREP_{UC}$ from UC to SM_k. Fig. 3 shows certificate verification process for EV_i authentication. Note that the public key $Pub^*_{EV_i}$ in $Cert^*_{EV_i}$ that is stored in VCL_k will be used by the SM_k for the EV_i's digital signature verification since $Cert_{EV_i}$ in $CREQ_{EV_i}$ has not been verified yet.

4.3 VCL Maintenance Scheme

VCL on each smart meter needs to be maintained periodically to remove expired certificates, revoked certificates, and temporary-event certificates (e.g., certificates from out-of-town EVs). Removing expired certificates is straight forward based on the expiration date without causing any additional traffic in the network. Removing revoked and temporary-event certificates however, introduce additional downlink traffic and periodic uplink traffic respectively as explained next.

Removing Revoked Certificates Each time a new CRL update is released by any participating CAs, the utility company creates a customized CRL for each gateway based on this new release. The revoked certificates information from multiple participating CAs can be combined into one customized CRL for each gateway. For each new revoked certificate in the new CRL update, the utility company searches the LCL to identify the gateway(s) of smart meters that keep it as a verified certificate in their VCLs. For each of these gateways, the utility company creates a customized CRL that contains only new revoked certificates for that gateway. Note that not all gateways will receive a customized

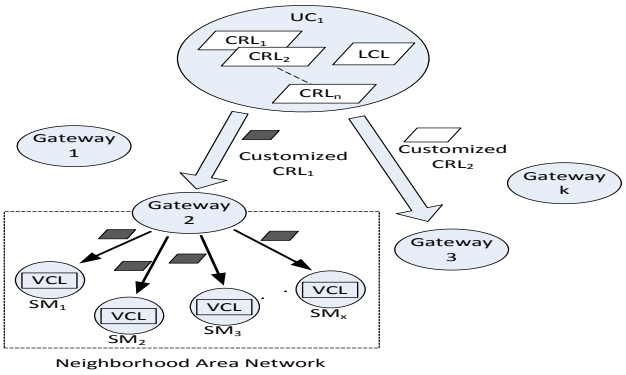


Fig. 4: Customized CRL creation and distribution for VCL maintenance.

CRL since this depends on whether there is a new revoked certificate that must be disseminated to that particular gateway. Thus, it can be considered as a randomly occurring event. Fig. 4 illustrates this distribution. On receiving a customized CRL, a gateway forwards it to all smart meters in the AMI. Every smart meter will update its VCL based on the received customized CRL.

Removing Temporary-Event Certificates A Least Frequently Used mechanism is proposed to keep track of the frequency of an EV communication to a smart meter within a time period T (e.g., every month). For each successful connection, the frequency of the corresponding certificate in VCL will be incremented. At the end of each period T, every smart meter will remove certificates from its VCL with a frequency less than a threshold β, where $\beta \geq 1$ and then the frequency attribute of remaining certificates will be reset. Thus, VCL always stores the frequently used certificates in that period only and avoids the previously dominating certificate usage to be carried over to the next period. Even though the Least Frequently Used mechanism can reduce the required storage space for a VCL, coherency issues may arise between VCLs and LCL. Therefore, the removed certificate(s) must be reported to the utility company to update the LCL.

5 Performance Evaluation

5.1 Baselines and Performance Metrics

We compared the performance of the proposed VCL with OCSP and the distributed CRL (D-CRL) that stores the certificates locally at each smart meter using the following metrics: (1) *Storage*, the space required to store the certificate and revocation information at smart meters; (2) *End-to-End Delay*, the delay incurred to verify an EV's certificate, which is the elapsed time between the first connection request sent by the EV and the connection reply the EV received; and (3) *Success Rate*, the ratio of the number of actual connection replies received by EVs to the total number of expected connection replies.

5.2 Experimental Setup

Two experiment scenarios are planned for performance evaluations. In both scenarios, the speeds of 40mph and 70mph are used assuming that EVs are in urban or highway environments when they need recharging. In the first scenario, the experiments are conducted in a controlled setup where EVs follow a straight path and start sending a connection request at the same time. 10 smart meters are chosen randomly from each topology representing the microgrids that periodically broadcast service messages to advertise their unit price for charging. A number of VpM (Vehicles per Meter) $\in \{2, 4, 5, 8, 10\}$ are placed at the very edge of the communication range of each of these microgrids. These vehicles broadcast their basic safety related messages periodically to surrounding vehicles. The simulation time is kept shorter (e.g., 20sec) since each EV goes out of the communication range of the associated smart meter. We assumed 20%, 40% and 60% miss rates where a valid certificate is searched in the VCL and does not exist there. These approaches are depicted as VCL-20%, VCL-40% and VCL-60% in the graphs. In such cases, the search is directed to the utility company.

In Scenario 2, the experiments are run in a more realistic environment using realistic traces that are generated in VanetMobiSim [22] by varying the number of vehicles and their speed. Thus, the amount of time an EV can stay within a smart meter's communication range varies. We assumed that 20% of the EVs need to recharge. The simulation time is 500sec to ensure that all of these EVs receive at least one broadcast service message and send a connection request. The experiment results are collected from 30 random mesh network topologies consisting of 81 nodes for statistical significance.

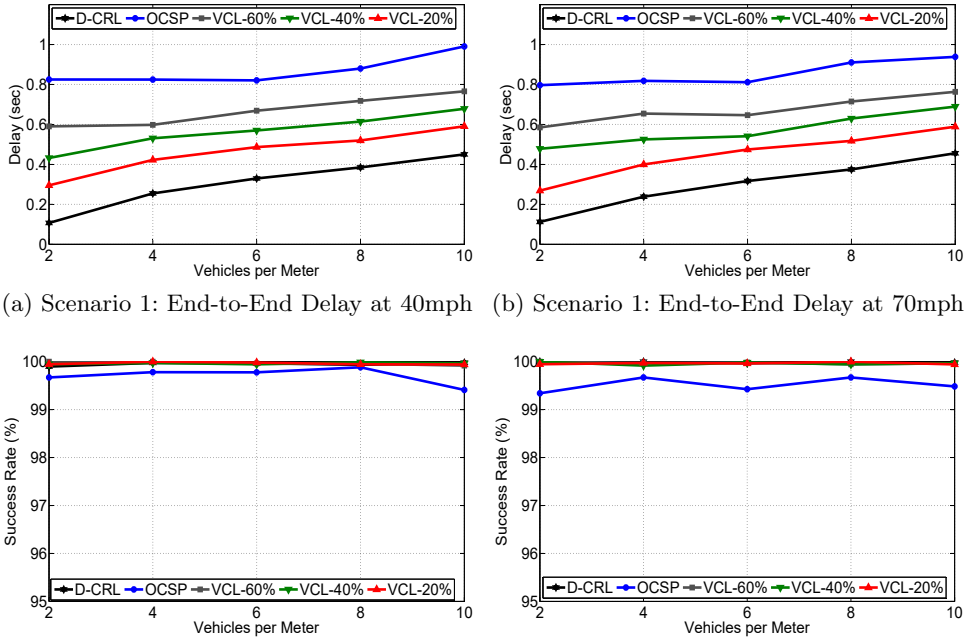
5.3 Performance Results

Storage Requirements Obviously, OCSP and D-CRL represent the two extremes of the required space in a smart meter. OCSP does not need any space in the smart meter since everything is stored at the certificate authority. Typically CRL only stores minimum information (e.g., certificate serial numbers) while a smart meter also needs the public key for authentication. Therefore, D-CRL stores both CRL and EV's certificates. Thus, the total storage needed for the D-CRL is the CRL size + certificate size. Depending on the number of revoked certificates, the average CRL size for V2V applications can become huge [23] (i.e., order of MBs). Even in case of EVs, there are around 500K EVs in the US now and a 100K revoked certificate will require around 6 MB storage space (each revoked certificate holds 68 bytes in CRL). VCL only needs to store the reduced customized EV certificate size (e.g., by omitting the certificate authority's digital signature (128 bytes), the typical 1024 bytes certificates will become 896 bytes). Assuming 1000 entries are kept in VCL, our approach requires around 900KB when D-CRL is used. A summary of comparison is given in Table 2.

Table 2: Storage overhead on smart meters.

Approach	List Entry	Certificate	Avg. Total
OCSP	0	0	0
VCL	4 bytes	896 bytes	900(KB)
D-CRL	20 bytes	1024 bytes	6.48(MB)

End-to-End Delay The simulation results for scenario 1 as shown in Fig. 5a and Fig. 5b indicate that speed of the vehicle does not affect the performance of the approaches significantly. The delay performance all approaches for 70 mph almost match the performance when the speeds are 40 mph. In general, since the vehicle density is kept same, 802.11p MAC layer can keep up with the speed.



(a) Scenario 1: End-to-End Delay at 40mph (b) Scenario 1: End-to-End Delay at 70mph

(c) Scenario 1: Success Rate at 40mph (d) Scenario 1: Success Rate at 70mph

Fig. 5: Performance metric comparisons for Scenario 1.

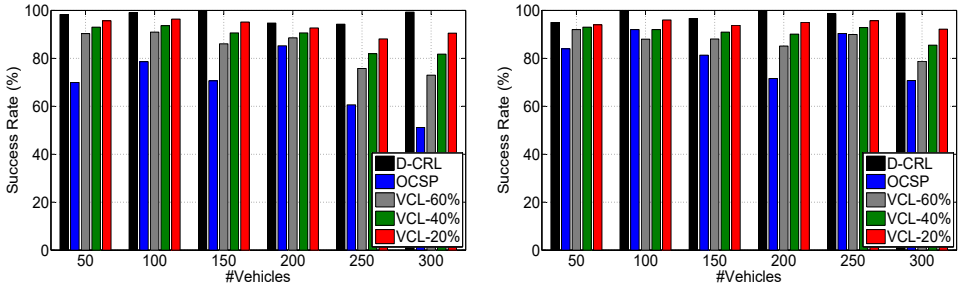
When looking at different approaches, VCL variants (VCL-20%, VCL-40%, VCL-60%) reduce the delay compared to OCSP. This is because of the network delay of OCSP for accessing the CRL at the certificate authority. In case of VCL, there can be misses which requires the smart meter to communicate with the utility company. This increases the delay slightly in the VCL but still it performs better than OCSP. D-CRL performs the fastest verification at the expense of not only the increased storage but also CRL maintenance that needs to be done from utility companies to smart meters. This is obviously another overhead for the

AMI network which does not exist for our approach. VCL minimizes the space requirements with a slight increase in End-to-End delay. However, this slight increase is due to mostly first time contact of smart meters from out of town EVs. For the frequent usage of EVs from the same neighborhoods, this delay will be further reduced.

Fig. 5a and Fig. 5b also indicate that as the number of EVs increases the delay increases for D-CRL. This is because the traffic over V2G is impacted from V2V communication. Since every vehicle broadcasts safety messages, this causes congestion on the channel. This observation shows that V2G communication has a communication latency and that verifying signatures from fast moving EVs become even more challenging in terms of latency requirements.

Success Rate The success rate values for Scenario 1 are given in Fig. 5c and Fig. 5d, respectively. As in End-to-end delay, there is no significant difference between the speeds in success rate values. The increase in number of vehicles very slightly deteriorates the success rate performance of D-CRL and the VCL variants. The performance of OCSP deteriorates a little bit more compared to the other approaches. This is because it is more probable for OCSP to miss a connection reply since the EV can go out of the smart meter's communication range before the reply arrives. Thus, the EV will need a reattempt.

Fig. 6a and Fig. 6b show the results for Scenario 2. The D-CRL approach outperforms the other approaches because it does not require to communicate with the mesh network and this reduces packet losses. The success rate values of our approach are slightly less than D-CRL values due to those EVs whose certificate information is not found in the VCL on the smart meters. This requires to contact the utility company, which consequently decreases the number of connection replies received. The success rate values for our approach decrease when the miss rate increases due to the same reason given in Scenario 1 results. The OCSP approach shows the worst performance as expected because it needs to contact the utility company at each time. Most of the time, the time interval in which the EV stays within a smart meter's communication range is not sufficient to receive a connection reply from the smart meter.



(a) Scenario 2: Success Rate at 40mph (b) Scenario 2: Success Rate at 70mph

Fig. 6: Performance metric comparisons for Scenario 2.

As can be seen in the bar graphs, the success rate values do not show a tendency and fluctuate. We attribute this to the traces that are completely independent of each other. The simulator created a new trace that is completely different than the previous one at each time we changed a parameter (the number of vehicles or the speed). Since it does not take the position of the smart meters into consideration while creating the traces, the smart meters with which the EVs interact and the round-trip time changes at each trace. This particularly affects the performance of the OCSP approach because the smart meter needs to contact the CA whenever a certificate verification is required.

6 Conclusion

In this paper, we have proposed an efficient certificate verification scheme for EVs-microgrids communications. Our network model uses the AMI networks as the communication network between EVs, smart meters and the utility companies. Using the traditional CRLs is not efficient because the smart meters need to maintain CRLs not just for the AMI network but also for a large number of EVs. These CRLs are long because each EV will use a large number of certificates to preserve privacy for V2V applications. We considered the case of EV to AMI communication through smart meters and introduced the idea of maintaining list of valid certificates. Our scheme maintains an up-to-date list of frequently used valid certificates. This idea is specifically interesting when EVs charge from the same places frequently.

We evaluated the performance of the proposed scheme through an implementation under ns-3 by using IEEE 802.11s, IEEE 802.11p and LTE standards. The results confirmed that the proposed approach significantly reduces the certificate verification time and the storage requirements on smart meters, and that it is highly reliable to be employed in realistic environments.

Acknowledgement

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000779.

References

1. Lund, H., Kempton, W.: Integration of renewable energy into the transport and electricity sectors through V2G. Energy policy 36(9), 3578–3587 (2008)
2. DoE: Alternative fueling station counts by state, alternative fuels data center, `http://www.afdc.energy.gov/fuels/stations_counts.html`
3. Hebner, R.: Nanogrids, microgrids, and big data: The future of the power grid. IEEE Spectrum Magazine (2017)
4. Networks, P.A.: Pan-os administrator's guide (2016), `https://www.paloaltonetworks.com/content/dam/pan/_US/assets/pdf/framemaker/61/pan-os/pan-os/section_3.pdf`

5. Wu, X., Subramanian, S., Guha, R., White, R.G., Li, J., Lu, K.W., Bucceri, A., Zhang, T.: Vehicular communications using DSRC: challenges, enhancements, and evolution. IEEE Journal on Selected Areas in Communications 31(9), 399–408 (2013)
6. Galperin, S., Santesson, S., Myers, M., Malpani, A., Adams, C.: X. 509 internet public key infrastructure online certificate status protocol-OCSP (2013)
7. Falk, R., Fries, S.: Securely connecting electric vehicles to the smart grid. International Journal on Advances in Internet Technology 6(1) (2013)
8. Pettersen, Y.: The transport layer security (TLS) multiple certificate status request extension (2013)
9. Zhang, Y., Gjessing, S., Liu, H., Ning, H., Yang, L., Guizani, M.: Securing vehicle-to-grid communications in the smart grid. Wireless Communications, IEEE 20(6), 66–73 (2013)
10. Vaidya, B., Makrakis, D., Mouftah, H.T.: Security mechanism for multi-domain vehicle-to-grid infrastructure. In: IEEE Global Telecommunications Conference (GLOBECOM 2011). pp. 1–5 (2011)
11. Vaidya, B., Makrakis, D., Mouftah, H.T.: Multi-domain public key infrastructure for vehicle-to-grid network. In: Military Communications Conference, MILCOM 2015-2015 IEEE. pp. 1572–1577. IEEE (2015)
12. Baumeister, T., Dong, Y.: Towards secure identity management for the smart grid. Security and Communication Networks 9(9), 808–822 (2016), http://dx.doi.org/10.1002/sec.996
13. Mültin, M., Schmeck, H.: Plug-and-charge and e-roaming–capabilities of the ISO/IEC 15118 for the e-mobility scenario. at–Automatisierungstechnik 62(4), 241–248 (2014)
14. Saputro, N., Akkaya, K., Uludag, S.: A survey of routing protocols for smart grid communications. Computer Networks 56(11), 2742 – 2771 (2012), http://www.sciencedirect.com/science/article/pii/S1389128612001429
15. Neichin, G., Cheng, D.: 2010 U.S. smart grid vendor ecosystem, https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/2010_U.S._Smart_Grid_Vendor_Ecosystem_Report.pdf
16. IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications amendment 10: Mesh networking. IEEE Std 802.11s-2011 pp. 1 –372 (10 2011)
17. Koohifar, F., Saputro, N., Guvenc, I., Akkaya, K.: Hybrid Wi-Fi/LTE aggregation architecture for smart meter communications. In: 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm). pp. 575–580 (Nov 2015)
18. Saputro, N., Akkaya, K., Tonyali, S.: Addressing network interoperability in hybrid IEEE 802.11s/LTE smart grid communications. In: 2016 IEEE 41st Conference on Local Computer Networks (LCN). pp. 623–626 (Nov 2016)
19. Akkaya, K., Rabieh, K., Mahmoud, M., Tonyali, S.: Customized certificate revocation lists for IEEE 802.11s-based smart grid AMI networks. IEEE Transactions on Smart Grid 6(5), 2366–2374 (Sept 2015)
20. Rabieh, K., Mahmoud, M., akkaya, K., Tonyali, S.: Scalable certificate revocation schemes for smart grid AMI networks using bloom filters. IEEE Transactions on Dependable and Secure Computing PP(99), 1–1 (2015)
21. Tonyali, S., Akkaya, K., Saputro, N.: An attribute-based reliable multicast-over-broadcast protocol for firmware updates in smart meter networks. In: 2017 IEEE

Conference on Computer Communications Workshops (INFOCOM WKSHPS) (May 2017)
22. Härri, J., Filali, F., Bonnet, C., Fiore, M.: Vanetmobisim: generating realistic mobility patterns for VANETs. In: Proceedings of the 3rd international workshop on Vehicular ad hoc networks. pp. 96–97. ACM (2006)
23. Khodaei, M.: Secure vehicular communication systems: Design and implementation of a vehicular PKI (VPKI) (2012)