Efficient Management of Certificate Revocation Lists in Smart Grid Advanced Metering Infrastructure

Mumin Cebe and Kemal Akkaya
Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174
Email: {mcebe—kakkaya}@fiu.edu

***Abstract*—Advanced Metering Infrastructure (AMI) forms a communication network for the collection of power data from smart meters in Smart Grid. As the communication within an AMI needs to be secure, key management becomes an issue due to overhead and limited resources. While using public-keys eliminate some of the overhead of key management, there is still challenges regarding certificates that store and certify the public-keys. In particular, distribution and storage of certificate revocation list (CRL) is major a challenge due to cost of distribution and storage in AMI networks which typically consist of wireless multi-hop networks. Motivated by the need of keeping the CRL distribution and storage cost effective and scalable, in this paper, we present a distributed CRL management model utilizing the idea of distributed hash trees (DHTs) from peer-to-peer (P2P) networks. The basic idea is to share the burden of storage of CRLs among all the smart meters by exploiting the meshing capability of the smart meters among each other. Thus, using DHTs not only reduces the space requirements for CRLs but also makes the CRL updates more convenient. We implemented this structure on ns-3 using IEEE 802.11s mesh standard as a model for AMI and demonstrated its superior performance with respect to traditional methods of CRL management through extensive simulations.**

I. Introduction

The existing power grid is currently going through a major transformation to enhance its reliability and efficiency by enabling networks of intelligent electronic devices, distributed generators, and dispersed loads [1] [2], which is referred to as *Smart Grid*. The concept utilizes advanced communication networks for management and coordination at different components of the Smart Grid such as power generation, transmission and distribution [3]. Advanced Metering Infrastructure (AMI) which is part of the Smart Grid distribution systems, is one of the renewed components of Smart Grid that collects smart meter data using a two-way communication network [3]. Smart meters are typically connected via a wireless mesh network with a gateway serving as a relay between the meters and the utility company. AMI network provides a multi-hop path towards the destination and thereby spanning longer distances for coverage. The advanced structure of AMI network is generally used to facilitate reduction of peak demand by monitoring the power demands over short periods and providing various rating and the effective management system based on remote metering data.

The security requirements for the AMI network are not different from the conventional networks as confidentiality, authentication, message integrity, access control, and non-repudiation are all needed to secure the collection of the customer's power data. Confidentiality is needed to prevent exposure of customer's private data to unauthorized parties while integrity is needed to ensure that power readings are not changed for billing fraud. Furthermore, authentication is crucial to prevent any outsiders impersonate the smart meters etc. As in the case of conventional network, these requirements can be easily met by using either symmetric or asymmetric key cryptography. However, in both cases management of the keys is a big issue in terms of automation, efficiency and cost. Due to the huge overhead of maintaining symmetric keys [4], using public-keys can provide some advantages and makes it easier to communicate with outside networks when needed [5].

However, adopting PKI for AMI poses challenges in terms of management of *certificates*, which are used to bind the certificate holder's identity to its public key. Specifically, the overhead of managing certificates on resource-constrained smart meters and utilities should be considered. The management of certificates typically refers to the creation, renewal, distribution and revocation of these certificates. Most of these tasks are done by Certificate Authorities (CAs) that act as third-party service providers. In particular, the certificate revocation is critical and has the potential to impact the performance of AMI applications significantly [6].

Therefore, there is a need to systematically manage the increasing size of the CRLs without causing too much overhead to distribute and store within smart meters. In this paper, we aim to develop customized solution for CRL management that will secure the communications in AMI. We strive to minimize the storage need of CRL by maintaining a distributed data structure called *Distributed Hash Table (DHT)* [7]. This study is the first study that utilizes the AMI network as a distributed infrastructure to provide scalable and efficient solution to CRL management problem considering the other duties of smart meters and reduce the CRL distribution and storage overhead significantly.

The performance of the proposed approach is assessed via simulations in ns-3 network simulator by implementing a wireless mesh network as an AMI that uses 802.11s and integrating AMI with the utility systems via LTE communication protocol. We compare our approach with the other methods that uses conventional CRL scheme, bloom-filters to speed

up the CRL search and OCSP. The simulation results shows that the proposed DHT-based CRL management overhead is much less compared the other methods. It not only reduces storage requirements on the smart meters but also decreases distribution overhead with reasonable access times regardless of the AMI network size.

This paper is organized as follows. In the next section, we describe the related works. Section III details the proposed approach. In Section IV, we present and discuss the experimental results and Section V concludes the paper.

II. Related Work

A. PKI for Smart Grid

The first study that focuses on the CRL management in Smart Grid was [6]. The authors investigated different CRL management aspects as short-lived-certificate scheme, tamper-proof device scheme, online certificate status server scheme, certificate revocation list (CRL), and compressed CRL in various applications of Smart Grid. The CRL management scheme based on Bloom Filters was proposed in [8]. The size of CRLs can be reduced by Bloom Filter which is a special data structure to store the CRL information and access it quickly. However, this data structure suffers from false positives and may eventually require accessing the actual server to check the validity of a certificate. Our scheme on the other hand never requires accessing a remote server. In [9], the authors proposed a CRL management scheme based on grouping the smart meters that are within the same neighborhood and likely to communicate. In the proposed scheme, smart meters only keep the CRL of its group to minimize the communication and storage overhead of CRL. While this approach is good for a specific application, it may limit the number of applications to be run on AMI infrastructure (i.e., Demand Response applications in AMI requires communication of any smart meters). Our proposed approach does not have such a limitation and can be used for any application.

B. Distributed Hash Tables

DHTs have been widely used in many applications and particularly in P2P networks [7]. There are also a number of studies proposing the use of DHT to manage CRL in large scale networks [10] [11] [12] [13]. However, these approaches mainly focus on the implementation of a distributed revocation system for P2P networks, such as BitTorrent or P2PStream. Our method leverages some ideas from these studies and propose a new distributed infrastructure to distribute and store CRLs over AMI. We use AMI network as an infrastructure and a service provider as a P2P network. In our approach smart meters work together to provide the certificate verification service in a distributed environment. Comparing the Internet-scale size and structure of a typical P2P network with AMI networks, the used DHT schemes in the previous P2P studies are not suitable for AMI. Therefore, we propose another DHT scheme that is based on Fibonacci numbers. As a result, we were able to obtain a significant reduction in both CRL distribution and storage overhead.

III. Proposed Approach

A. Overview

As mentioned, the problem of certificate revocation introduces a lot of overhead with the increased network size. In addition, the size of the CRL can become quite large, which hinders their distribution. Our proposed approach to this problem utilizes the concept of DHTs offered in [7]. Referred to as *Chord*, such use of DHTs decreases the cost of storing and distributing CRL and provide scalability by keeping the cost of validating the status of certificates low enough.

Inspired from this idea, the central concept of our approach is to divide the entire CRL into several portions in order to avoid unmanageable CRL size for the smart meters. Chord builds a data structure to provide us to divide CRL in to several small portions. Chord mainly requires each item to be stored in DHT to be unique. This is a requirement for spreading keys uniformly across the imaginary ring which helps for uniformity while mapping both node IDs (in our case IPs) and keys (in our case certificate IDs) to same circular space. The uniqueness constraint is perfectly fit to our problem since we will store revoked certificate IDs which are unique. These CRL portions are kept and shared in a distributed way where all smart meters are considered as potential servers of CRL portions, and the gateway acts like distributor of CRL portions. Each smart meter will just keep one portion of CRL and will use a finger table to find other CRL portions when it is required. This finger table will help smart meters work together to find out whether a certificate is revoked or not.

B. CRL Partitioning

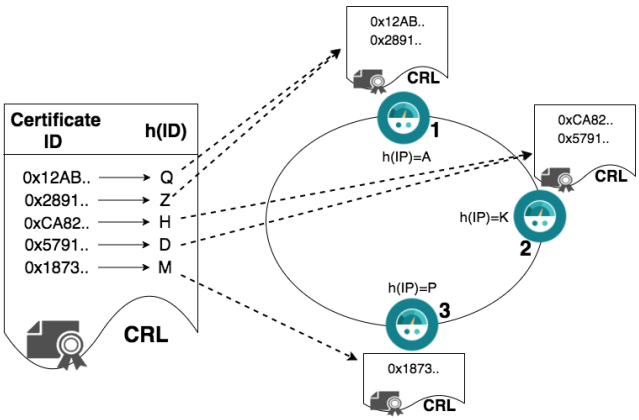

Fig. 1: CRL Partitioning

CRLs are divided into N portions where N is the number of smart meters within the AMI. To that end, CAs use a consistent hash function [14] to determine the corresponding portions of a certificate serial number. In this way, each time the CA revokes a certificate, it calculates the hash of the certificate serial number and stores it in the CRL portion determined by

output of it. Note that consistent hashing is used to ensure that both keys and IP addresses are uniformly distributed in the same identifier space.

Figure 1 shows an example on how a CRL is partitioned into 3 CRL portions according to this scheme. Smart meters are located on an imaginary ring according to $h(k)$ which maps the IP addresses to a letter. In addition, each certificate ID is mapped to a letter using $h(i)$. The certificate ID 23 would be kept in the CRL portion that belongs to smart meter 2 since $h(23) = H$ is in between A and K. Similarly, the certificate ID 11 would be located in CRL portion that belongs to smart meter 1 since corresponding hash value of $h(11) = Q$ is in between P and A in the ring topology and the remaining are located in the same way.

C. CRL Lookup

Chord will decrease the CRL size at the expense of additional lookup cost arising from sending lookup messages through the AMI network. Checking a certificate ID from Chord requires reaching the responsible smart meter via a routing operation. This lookup is accomplished by a *finger table* scheme. However, the finger table scheme of Chord is optimized for P2P networks which may have have millions of nodes. Considering size of AMI (hundreds to thousands), which is smaller than a typical P2P network, it does not provide an optimal trade-off between resources exploited and performance.

Thus, we use another routing scheme which is proposed in [15]. This study defines an improved finger table based on Fibonacci distances where the objective is to reduce the number of hops, possibly at the expense of an increased size of the finger table. In this routing scheme, each node in the network keeps some of its successors' identities which maintain a finger table where the i^{th} entry of finger table of n^{th} node is the successor of $n + G_k(i)$ on the ring. For a given key, routing will be done comparing the entries on the finger table and the node forwards the message to the successor that is closest to the key but not greater than the key. G_k recursively defines a family of "Fibonacci" sequence members and constructs a finger table which includes the address of the peer that is located at distance $G_k(i)$ in terms of the number of hops in the ring structure from the local node as follows:

$$\forall k \in IN, \forall i \in IN : i \geq k, G_k(i+1) = G_k(i) + G_k(i-k)$$

where $\forall i \leq k,\ G_k(i) = 1$ as the initial condition. This creates "usual Fibonacci" sequence in case $k = 1$ and special fibonacci sequences where $k > 1$. Following this idea, we can thus define a finger table, which includes the address of the smart meters that is located at distance $G_k(i)$ in terms of the hop count in the ring structure from the local node, as the i^th element of its table.

IV. Performance Evaluation

A. Experimental Setup

To evaluate the performance, we used network simulation to create a wireless mesh-based AMI network. The proposed approach is developed under NS-3 simulator which has a built-in implementation of IEEE 802.11s. The underlying MAC protocol used was 802.11g. The gateway was integrated with the utility systems via LTE which was also implemented in NS-3 for testing the cases where there will be access to outside servers. We created two different grid topologies that consists 81 and 196 smart meters, respectively. We assumed a transmission range of 120 m and create grid topologies according to this range. A gateway is selected at the upper-left corner of the grid. The smart meters are assumed to generate power readings at certain intervals and create a packet size of 512bytes. The certificates are created using OpenSSL. We also prepared a DER (binary) encoded CRL list that has been digitally signed according to RFC 5280 which contains 90K revoked certificates.

B. Baseline and Performance Metrics

We considered the following three performance metrics to assess the network performance for the CRL management:

- *Average number of Packets*: This metric indicates the average number of messages received and processed by a smart meter. This metric will show how much data is transmitted in the network and thus hints about the bandwidth usage.
- *Average Packet Delay*: This metrics measures the time it takes for each message to reach the intended smart meter during CRL distribution.
- *Total Time*: This metric indicates the total elapsed time to complete the CRL distribution process.
- *CRL Storage*: This metric indicates the total required storage space for each smart meters
- *CRL Lookup Time*: This is the average lookup time to check whether a certificate ID is revoked or not. This relates to network delay when a server is accessed, it does not consider the local search time in the file as this is ignored.

We compared the performance of the proposed approach with two other cases. In the first case, we assume that each smart meters keeps the whole CRL locally. In the second case, a bloom filter is used to store revoked certificates information. Furthermore, a number of experiment scenarios are planned for performance evaluation of CRL distribution and CRL lookup for each of these cases when applicable. We detail these scenarios below.

1) Distribution of CRL: In the first scenario, we compressed the CRL file and distribute it to smart meters over the gateway. The gateway distributes the CRL by unicasting to the each smart meters. However, this is a costly process in terms of the required bandwidth and time since it is literally sending the same data for over and over again.

Therefore, for the second scenario, we use broadcasting and apply random linear network coding technique [16] to increase the network bandwidth efficiency. To distribute CRL by linear network coding, the compressed CRL file is divided into generations and each generation contains same number of k packets denoted p_i, $i = 1, 2, ..., k$, which are d bytes

TABLE I: Distribution Overhead-Network Coding-AMI-81

Broadcast Interval		Local CRL	Bloom Filter
0.1 Second	Avg # Packets	2029.47	222.85
	Avg. Packet Delay (s)	0.29	0.29
	Avg. Total Time (m)	7.5	0.82
0.5 Second	Avg # Packets	1582.13	173.73
	Avg. Packet Delay (s)	0.19	0.18
	Avg. Total Time (m)	11.67	1.28

TABLE II: Distribution Overhead-Network Coding-AMI-196

Broadcast Interval		Local CRL	Bloom Filter
0.1 Second	Avg # Packets	2880.54	316.30
	Avg. Packet Delay (s)	0.47	0.47
	Avg. Total Time (m)	10.67	1.17
0.5 Second	Avg # Packets	1571.20	172.50
	Avg. Packet Delay (s)	0.32	0.31
	Avg. Total Time (m)	12.5	1.37

each. Each packet is broadcast through the gateway with an encoding vector header.

In the third scenario, we use Bloom filter to store the revoked certificates information. To do so, we read previous CRL file and we insert each revoked ID to a Bloom filter by discarding the revocation date information. However, Bloom filter allows to reduce false positive rates below a certain level by sacrificing its storage advantage [17]. Therefore, we assumed that 1% error rate is acceptable for our scenario and built a typical Bloom filter with 1% error rate. We signed the formed Bloom filter and distribute it by using both unicast and linear network coding similar to previous scenarios.

As the final scenario, we consider our proposed case where finger table parameter k is selected as 3 and 5 for AMI-81 and AMI-196, respectively. Since each CRL portion is different from each other, we only use unicast through the gateway to send CRL portion and finger table to the related smart meter.

2) CRL Lookup: We assume that each smart meter has already got required CRL information and 10% of randomly chosen smart meters need CRL lookup at the same time. We compare our approach to the two other baselines mentioned in terms of required space to keep CRL information and the elapsed time to check whether the certificate is valid or not. Note that we use just network delay as a search metric since the search time in the local list depends on the used data structure, search algorithm, storage and CPU capabilities of the smart meter for all approaches. For this reason, we simply neglect the required local search time and focus on required network delay metric.

C. Experiment Results

1) CRL Distribution Overhead: We first conducted experiments to assess the CRL distribution overhead of the proposed approach. We used four different time intervals as 0.1 and 0.5 second between broadcast messages while distributing CRL. As noted before for DHT, we did not use broadcasting and thus only unicast results will be discussed.

TABLE III: CRL Distribution Overhead-Unicast

	DHT	Local CRL	Bloom Filter
# Packets	14/6*	1092	120
Avg. Packet Delay (s)	0.03/0.06*	0.13/0.19*	0.12/0.19*
Avg. Total Time (m)	0.32/0.35*	25.5/33.3*	2.8/3.6*

* results for AMI-81 and AMI-196, respectively

The message overhead for all the approaches are shown in Tables I, II and III. The results indicate that DHT reduces the message overhead significantly compared to Bloom filter and local CRL approaches due to partitioning. This is also apparent even if broadcasting is not used in the case of Bloom filter and local CRL approaches. Another observation is that, decreasing broadcast interval helps to decrease the total time. However, this cause the average packet delay and average number of packets to increase. As seen from Table I and II, the packet delay increases up to 0.47 seconds. This can be attributed to the fact that there will be more contention and congestion in the network and even some of the packets may be dropped and resent. However, in average the total time will be decreasing since the packets are generated faster. Although faster generation helps to complete the whole process earlier, the average packet delay is dependent on the network size. As seen in Table II, the delay increases compared to the delay shown in Table I but the increase is not linear. Thus, for large scale networks, the broadcast interval should be selected carefully to avoid to much congestion.

Looking at the unicasting results in Table III, we see that the results are encouraging since our DHT-based approach still outperforms the others and provides significant reductions in terms of packet delay, number of packets and total completion time of the distribution. According to these results, the average total time for the local CRL and bloom filter approaches is increasing at a faster rate than DHT which hints about the scalability of our approach. DHT approach has better scalability due to the fact that it is not affected from the network size. This make DHT even a better candidate to be employed.

2) CRL Storage and Lookup Overhead: To compare the storage requirements, we identified the needed CRL size for our approach and compared with the other baselines. Table IV shows the comparison of these approaches. As expected, DHT needs store a small portion of CRL since the whole CRL list is distributed to smart meters in nearly equal portions. However, local CRL keeps the whole CRL list and depending on the number of revoked certificates, it can be huge. For our scenario, the CRL size is nearly 2MB for 90K revoked certificates. DHT only needs to store nearly $1/N$ of CRL size which is around 30KB and 10KB. While Bloom filter's performance is also promising, it may suffer from false positives as discussed before.

Looking at the Lookup delay for the CRL, as expected, there is no delay for local CRL approach (other than the negligible search time within the file). The Bloom filter is also pretty fast but in case of false positives, it suffers from increased

TABLE IV: CRL Lookup Overhead

	Local CRL	**Bloom Filter**	**DHT**
Required Space (mb)	2.18	0.12	0.03/0.01*
Network Delay (s)	0	0.48/0.55*	0.01/0.03**

* results for AMI-81 and AMI-196, respectively
** delay after path discovery for AMI-81 and AMI-196, respectively

network delays to access a remote server which increases the average delay. Our proposed approach brings more delay since the lookup time needs to access smart meters which requires transmission of queries over the mesh network. However, this time is very reasonable and still less than Bloom filter approach if the path is already known as shown in Table IV. As can be seen from the table, it is slightly effected from the network size.

3) CRL Update Overhead: In this section, we discuss how CRL updates are affected with our approach. We assume that the CRLs are updated regularly by using *delta CRL* concept. To assess the overhead of delta CRL updates, we assume that the delta CRL contains just one revoked certificate information and as a result it is 436 bytes.

For the local CRL approach, as in the case of full CRL distribution, every smart meter should store the delta CRLs locally, and thus our specific delta CRL file should be distributed to all smart meters. Therefore, the overhead of CRL distribution will be proportional to the size of delta CRL and according to that size the burden can be inferred by using the Table I and II. Thus, delta CRL will reduce the distribution overhead for local CRL approach. However, delta CRL concept does not bring any advantage to the Bloom filter approach. For each updated revocation information, the bloom filters must be created again from the scratch by using all revocation information to carry both previous and new revoked certificates. As a result, updating the CRL will have almost the same CRL distribution overhead as seen in Table I and II.

The only approach that brings an advantage to delta CRL concept is our approach. As in the case of full CRL, we will partition the delta CRL and distribute these to smart meters. However, for this special case, we do not need partitioning since it contains just one entry. According to the process, the certificate ID will be used determine the location of the delta CRL. Therefore, the delta CRL will be sent to a specific smart meter. As a result, the overhead will be updating one smart meter with one delta CRL. Thus, our approach provides superior results compared to the other approaches.

V. Conclusion

Considering the overhead of certificate and CRL management in AMI networks, in this paper, we proposed a DHT-based algorithm for creating and distributing the CRLs in an 802.11s-based AMI. Our approach strives to exploit the capabilities and resources of all the smart meters so that they accomplish CRL management in a collaborative and distributed manner. Basically, DHT structure is used to access the CRLs when a certificate is to be queried. In this way, the size of CRL was significantly reduced.

We implemented the proposed DHT-based approach in NS-3 simulator that runs a version of 802.11s. The experiment results indicate that the DH-based approach can reduce the CRL size significantly which helped reducing the distribution and the storage overhead in resource limited smart meters when compared to two other existing CRL management approaches.

Acknowledgement

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

References

[1] H. Liang, B. J. Choi, A. Abdrabou, W. Zhuang, and X. S. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, 2012.

[2] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, 2010.

[3] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, no. 11, 2012.

[4] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 30, no. 3, 2007.

[5] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, 2010.

[6] M. M. Mahmoud, J. Mišić, K. Akkaya, and X. Shen, "Investigating public-key certificate revocation in smart grid," *IEEE Internet of Things Journal*, vol. 2, no. 6, 2015.

[7] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, 2001.

[8] K. Rabieh, M. Mahmoud, S. Tonyali *et al.*, "Scalable certificate revocation schemes for smart grid ami networks using bloom filters," *IEEE Transactions on Dependable and Secure Computing*, 2015.

[9] K. Akkaya, K. Rabieh, M. Mahmoud, and S. Tonyali, "Efficient generation and distribution of crls for ieee 802.11 s-based smart grid ami networks," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014.

[10] G. Ying and Z. Jiang, "Research on crl distribution in p2p systems," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*. IEEE, 2009.

[11] J. Huang, Z. Wang, Z. Qiu, and M. Chen, "Theoretical analysis of issuing mechanism in distributive digital certificate revocation list," in *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*. IEEE, 2008.

[12] M. C. Morogan and S. Muftic, "Certificate revocation system based on peer-to-peer crl distribution," in *Proc. of the DMS'03 Conference*, 2003.

[13] A. Avramidis, P. Kotzanikolaou, C. Douligeris, and M. Burmester, "Chord-pki: A distributed trust infrastructure based on p2p networks," *Computer Networks*, vol. 56, no. 1, 2012.

[14] D. Karger, E. Lehman, T. Leighton, R. Panigrahy, M. Levine, and D. Lewin, "Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the world wide web," in *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*. ACM, 1997.

[15] G. Chiola, "Extended fibonacci distances for fault-tolerant routing in chord-like dhts," in *Peer-to-Peer Systems, 2004. International Workshop on Hot Topics in*. IEEE, 2004.

[16] Z. Yang, M. Li, and W. Lou, "A network coding approach to reliable broadcast in wireless mesh networks," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2009.

[17] F. Bonomi, M. Mitzenmacher, R. Panigrahy, S. Singh, and G. Varghese, "An improved construction for counting bloom filters," in *European Symposium on Algorithms*. Springer, 2006.