Efficient Public-key Revocation Management for Secure Smart Meter Communications using One-way Cryptographic Accumulators

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, public-key cryptography can be used to reduce the overhead of key management. However, it still has certain challenges in terms of certificate revocation and management. In particular, distribution and storage of the Certificate Revocation List (CRL), which holds the revoked certificates, is a major challenge due to its overhead. To address this challenge, in this paper, we propose a novel revocation management scheme by utilizing cryptographic accumulators which not only reduces the space requirements for revocation information but also enables convenient distribution of revocation information to all smart meters. We implemented this one-way cryptographic accumulator-based revocation scheme 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.**

***Index Terms*—AMI, one-way cryptographic accumulator, certificate revocation lists, Public Key Infrastructure**

I. Introduction

The existing power grid is currently going through a major transformation to enhance its reliability, resiliency and efficiency by enabling networks of intelligent electronic devices, distributed generators, and dispersed loads [1] [2], which is referred to as *Smart(er) Grid*. Advanced Metering Infrastructure (AMI) network is one of the renewed components of Smart Grid that helps to collect smart meter data using a two-way communication [3]. Smart meters are typically connected via a wireless mesh network with a gateway (or access point) serving as a relay between the meters and the utility company.

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 customers' power data [4]. As in the case of conventional network, these requirements can be met by using either symmetric or asymmetric key cryptography. However, in both cases, the management of the keys is a major issue in terms of automation, efficiency and cost. Due to the huge overhead of maintaining symmetric keys [5], using public-keys can provide some advantages and makes it easier to communicate with IP-based outside networks when needed [6].

However, adopting a public-key infrastructure (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. Therefore, the overhead of managing certificates on resource-constrained smart meters and utilities should be considered. In particular, the certificate revocation is critical and has the potential of significantly impacting the performance of various AMI applications from outage management to demand response [7]. Therefore, we focus on the management of certificate revocation.

There are several reasons that require revoking certificates such as key and certificate compromise, or excluding malicious meters. Note that, there were several recent incidents that required revoking of the certificates such as renowned heartbleed vulnerability [8] and latest RSA key generation chip-deficiency [9], which affected more than 700K certificates. As a result, a common practice is to perform a certificate status check before accepting it. Such check is typically done by looking up a Certificate Revocation List (CRL) which is used to store revoked certificates' serial numbers and revocation dates. The CRL size will grow significantly as time passes due to fact that the expiration period of a certificate is relatively longer than that of other conventional systems. The CRLs are typically stored locally in smart meters which have limited resource. This creates a trade-off between the size of the CRLs and storage space. In addition, distributing the CRLs is critical and will cause a significant burden over AMI infrastructure.

An alternative method would be to store the CRL in a remote server as in the case of Online certificate status protocols (OCSPs) [10] [11]. Thus, each time a query is sent to the server to check the status of the certificate. While OCSP-like approaches can be advantageous on Internet communications, employing them for AMI is not attractive since it will require access to a remote server which may be hosted outside of the utility network and may not be readily accessible.

Therefore, there is a need to develop a lightweight solution to manage the revocation information without causing too much overhead to distribute and store them within smart

meters. In this paper, we propose an efficient revocation scheme by using RSA cryptographic accumulators to replace CRLs [12]. The idea of a cryptographic accumulator is based on a group of honest members (i.e., *whitelist*) that hold the result of an accumulated hash (i.e., accumulator) and a membership witness. When needed, any of the group members can verify another member by using its membership witness and owned accumulator value. Cryptographic accumulators are space efficient and secure since finding membership witnesses for elements not in the group are computationally infeasible.

In the CRL case, however, we need to verify non-membership of a certificate (i.e., blacklist). Thus, the utility company will play the role of the accumulator manager to collect all publicly available CRLs from the different certificate authorities (CAs) and accumulate them to calculate a single accumulator value. This single short accumulator value will be used to update non-membership witness values of smart meters to provide a revocation mechanism. We define additional batch calculator function for the proposed accumulator scheme to calculate accumulation value in batch to provide lower communication cost. Finally, we define new roles within an AMI network to implement this idea.

The performance of the proposed approach is assessed via simulations in ns-3 network simulator by implementing an IEEE 802.11s-based AMI network that has a gateway which is connected to the utility systems via LTE communication protocol. We compared our approach with the other methods that use conventional CRL schemes and Bloom-filters [13], [14]. The simulation results show that the proposed revocation scheme overhead is much less compared to the other methods. It not only reduces storage requirements on the smart meters but also decreases distribution overhead.

This paper is organized as follows: In the next section, we summarize the related work. Section III provides the background and the system/attack models. In Section IV, we present the proposed accumulator with its features. Section V is dedicated to experimental validation. The paper is concluded in Section VI.

II. Related Work

A. Cryptographic Accumulators

Cryptographic accumulators were first introduced by Benalog and DeMare [15]. After their first appearance in the literature, they have been used in many applications [16] [15] [12] [17], including membership testing, time stamping, authenticated directory, and certificate revocation.

Recently, more efficient accumulator mechanisms have been proposed [18] [19]. For instance, Leonid and Yakoubov relaxed the frequent update requirement by introducing an asynchronous accumulator that helps to postpone updates to some extent [18]. Furthermore, the accumulator in [19] completely removes the update requirement when it is used just for non-membership proof. The scheme only needs to update accumulator value and membership witnesses when an element is removed from the list. Although this study achieves more efficient revocation mechanism from the previous studies, as the scheme is based on accumulating a valid list, it has some drawbacks in our AMI context. First, as revocation frequency and number of revoked certificates are less than new certificate registration and number of valid certificates [8], respectively, accumulating of the valid smart meters will still constitute a significant overhead. Second, smart meters are expected to interact with other devices such as smart appliances, electric vehicles, water and gas meters and that may require to obtain valid lists from corresponding vendors which will not be publicly accessible. Our approach alleviates these two concerns by utilizing CRLs.

B. CRL Management in AMIs

Due to increasing interest in Smart Grid, there has been a number of efforts to study PKI for Smart Grid communication infrastructure. For instance, Metke et al. [6] surveyed the existing key security technologies for extremely large, wide-area communication networks and claimed that the most effective key management solution for securing the Smart Grid in general will be based on PKI. Mahmoud et al. [20] focused on different aspects of PKI and in particular certificate revocation problem in Smart Grid. The authors in [7] investigated different CRL management aspects such as short-lived-certificate scheme, tamper-proof device scheme, OCSP, CRL, and compressed CRL in various applications of Smart Grid. However, these works do not provide a customized solution for AMI networks.

The first study that focused on the CRL management for AMI was based on Bloom Filters [13]. The size of CRLs was reduced by Bloom Filters which are special data structures for quick access. However, Bloom Filters suffer from false positives and may eventually require accessing the actual server to check the validity of a certificate. Our proposed scheme on the other hand never requires accessing a remote server. In [14], the authors proposed a CRL management scheme based on grouping the smart meters that are within the same neighborhood and likely to communicate with each other. 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 Our proposed approach does not have such a limitation and can be used for any application.

III. Preliminaries

A. Background on Cryptographic Accumulators

Cryptographic accumulator is a condensed representation of a set of elements [15]. It provides an efficient mechanism to check whether an element is a member of a set without revealing the other members' information. There are several known cryptographic accumulator constructions, the RSA construction, the Bilinear Map construction, and the Merkle Hash Tree construction are the most used ones. In our study, we employ the RSA construction approach, because of the space limit, the details of the approach will be provided whenever needed.

Benaloh and De Mare proposed using quasi-commutative property of one-way cryptographic accumulators to provide membership proof. An example of the quasi-commutative property of one-way accumulators is given in equation 1.

$$h(h(s_k, y_1), y_2) = h(h(s_k, y_2), y_1) \quad (1)$$

Specifically, when you start with one value inside of a set, which is called accumulator key s_k and a set of values y_i, the resulting accumulated hashes of these values stay the same even if the order of hashing is changed. For a membership test, imagine there is a group of users that hold the result of an accumulated hash value a which is computed from the set of $y_{1..m}$ values. Note that, the value of a does not depend on the order of y_i accumulations. This scheme is used for generating witness value w_j of corresponding y_j by accumulating all y_i such that $i \neq j$. Then, when necessary any of the users can authenticate one another by checking whether $h(w_j, y_j) = a$. Since h is a one-way function, it would be computationally infeasible to obtain w_j from y_j and a.

Although the first design of accumulators provides a condense way of membership testing, witness values should be calculated from scratch whenever there is an update on the accumulated list.The first form of one-way accumulator that supports computing without beginning from scratch is offered in [12] which is based on modular exponentiation with an RSA modulus. We now define the provided high level functions to construct an RSA accumulator as follows:

RSA Accumulator: Z_n represents all relative of prime numbers of an RSA modulus $N = pq$, where p and q are strong primes. Exponentiation in Z_n is one-way quasi-commutative and is used to construct a cryptographic accumulator as follows where inputs to the accumulated list is $x, y \in Z_n$

- $s_k, a_0 \leftarrow G(1^k)$: Takes a security parameter k (represents the length of s_k in bits) and initiates secret key of accumulator $s_k \in Z_n$ and accumulator value a_0.
- ${w_u}^t, a^t, {w_y}^t \leftarrow Add(a^{t-1}, y)$: Add element y to the accumulator a_{t-1} and returns witness update value ${w_u}^t$, new accumulator value a^t and witness value ${w_y}^t$ of y.
- ${w_x}^t \leftarrow WitnessUpdate(a^t, {w_u}^t, x)$: Takes newly generated ${w_u}^t$, accumulator value a^t, element x and returns witness value ${w_x}^t$ of element x after element y is added.
- $0, 1 \leftarrow Verify(a^t, x, {w_x}^t)$: When element x wants to authenticate itself to a third party, third party uses ${w_x}^t$ and a^t to check whether x is in the accumulated list.

B. Certificate, CRL and Delta CRLs

As we deal with certificates, we would like to also provide some basic background on certificates and their management. Certificates are issued by a CA with a planned lifetime to an expiration date and have unique serial numbers. A certificate may be valid from 1 minute to twenty years. Once issued, it is valid until the expiration date. However, there are various reasons that cause a certificate to be revoked before the expiration date. Some of these reasons include, but not limited to compromise of the corresponding private key, change of association between CA, general incidents, etc.

Revocation causes each CA regularly issuing a signed list called a CRL which is a time-stamped list consisting of serial numbers of revoked certificates and revocation dates. When a PKI-enabled system uses a certificate (for example, for verifying integrity of a message), that system should not only check the time validity of the certificate, but an additional check is required to determine a certificate's revocation status during the integrity check. To do so, the CRL can be accessed to determine the status of the certificate. A CA issues a new CRL either on a pre-configured regular periodic basis (for example, hourly, daily, or weekly) or on an event basis; for example, when an important certificate is compromised.

C. System and Attack Model

We assume that smart meter data collection and communication is done through a wireless mesh network (e.g., IEEE 802.11s or Zigbee). The gateway node which is connected to the utility company via 4G/LTE acts as the root node of the wireless mesh network.

For the attack model, we assume the followings: 1) In an attacker's perspective the meter is the entry point to the AMI. The attacker can compromise a certificate which can be used to force a malicious smart meter to connect to the AMI network; 2) The gateway is also assumed to be physically exposed to attackers. Moreover, it bridges the utility and other smart meters. If the certificate is compromised, the attackers might impersonate the gateway and apply different attacks. 3) Compromising the servers calculating accumulator values could expose all consumers' information.

IV. Proposed Approach

A. Adaptation of RSA Accumulator

Although RSA accumulator described in the previous section can provide very efficient *membership test* (i.e., whitelist), we need an accumulator scheme that provides a *non-membership test* (i.e., blacklist) to allow working with conventional CRLs where a certificate is deemed valid if it is not in the CRL. It is important to note that membership proof on black-list cannot be used for this purpose. This is because, we are looking for a non-membership proof.

To enable an accumulator with non-membership proof capability, we condense the serial numbers of revoked certificates in all CRLs within a short accumulator and construct the accumulator using the following functions:

- $v_{aux}, s_k, a_0 \leftarrow Generation(1^k)$: Takes a security parameter k (represent length of the secret key in bits) and initiates secret key s_k, accumulator value a_0 and auxiliary value v_{aux} which is used in non-membership verification.
- ${nw_u}^t, a_t \leftarrow NonMemberAdd(a^{t-1}, y)$: Add element y to the accumulator a^{t-1} and returns non-membership witness update value ${nw_u}^t$ and new accumulator value a^t.
- ${nw_x}^{t+n} \leftarrow NonMemWitBatch(a^{t+n}, {nw_u}^{(t..t+n)}, x)$: Takes a set of non-membership update values from t to $t+n$, latest accumulator value a^{t+n}, element x and returns non-witness value ${nw_x}^{t+n}$ of element x after bunch of

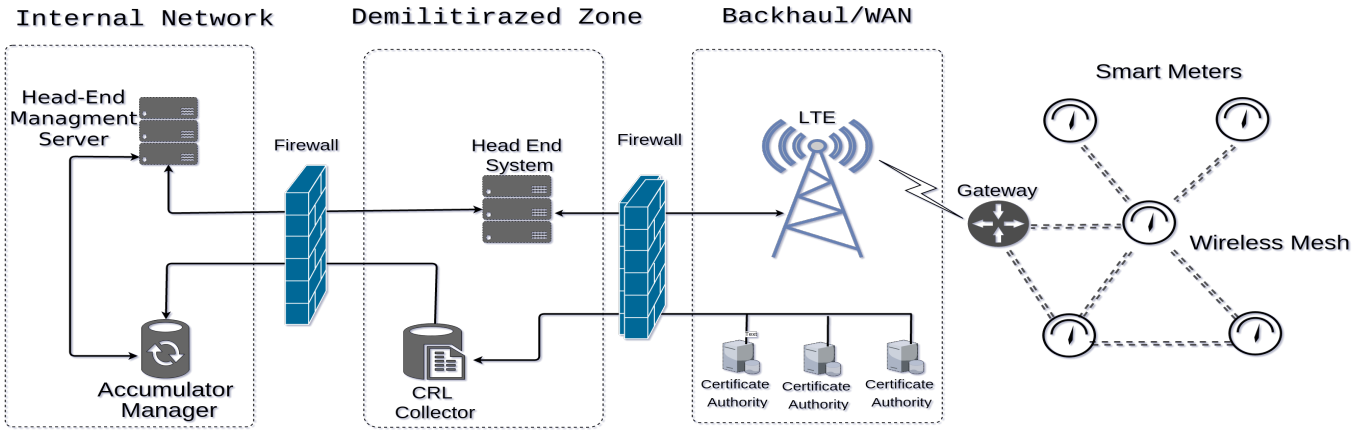

Fig. 1. The structure of proposed revocation management using cryptographic accumulators.

certificates revoked. This functionally is important when a general deficiency that requires revoking a large set of certificates.

- $0, 1 \leftarrow NonMemberVer(v_{aux}, a^t, x, {nw_x}^t)$: When element x wants to authenticate itself to a third party, third party uses v_{aux}, ${nw_x}^t$ and a^t to verify x is *not* in the accumulated revocation list.

This RSA accumulator provides a very efficient non-membership test by condensing a blacklist into a short accumulator. From the security perspective, the scheme has *correctness* since it always allows to verify a non-membership as long as the accumulator value is up-to-date. It is also *sound*, because it is hard obtain a non-witness value nw_x for a value x which is accumulated before.

Using this accumulator, we now build an efficient mutual authentication and revocation management system for AMI. Next, we define the components of the proposed scheme.

B. Components of Revocation Management System

We propose the system architecture shown in Figure 1 to enable efficient revocation management. The components of this architecture and their roles are described as follows:

- *Smart Meters:* The smart meters can directly communicate with the Head-end System (HES) over a gateway. A smart meter may also act as relay in order to route packets from other smart meters. Thus, smart meters need to support the *NonMemberVer* function for a complete mutual authentication mechanism.
- *Gateway:* The gateway serves as the interface between the HES and meters. Similar to smart meters, it needs to support *NonMemberVer* for mutual authentication. In addition, the gateway will also serve the other smart meters as supplying their calculated nw^t values with using *NonMemWitBatch*. The required set of non-witness update messages ${nw_u}^{(t..t+n)}$ is supplied from *Accumulator Manager*.
- *Head-End System:* The HES is located within utility company network to provide direct communication with the smart meters. Since it is an interface between utility company and smart meters, it is located in a demilitarized zone (DMZ). The primary function of the HES is collecting the power data from smart meters and transfer them to head-end management servers. In addition to this primary function, HES sends data (e.g., updated accumulator value) and commands to the smart meters. Since it has two-way communication with smart meters, it requires implementation of *NonMemberVer* function.
- *CRL Collector:* The CRL collector plays one of the key roles in our revocation management system. It basically collects CRLs from various CAs and feed them to the accumulator generator. Since it has open interface to outside network (communicating with other CAs), it is placed in DMZ area.
- *Accumulator Manager:* Accumulator Manager is the core of our revocation management scheme. It gets CRL information from the CRL Collector and accumulates them to obtain latest accumulator value. It implements the *Generation* and *NonmemberAdd* functions. Whenever a new accumulator value is calculated at time t, it sends accumulator value a_t and a set of non-witness update messages ${nw_u}^{(t..t+n)}$ to the head-end management server (HMS). HES will start distribution of these values to the gateways as soon as it is informed by the HMS.
- *Head End Management Server:* The collected data is managed within HMS. It basically monitors activity logs, identifies new devices and manages incident response processes. In our revocation scheme, the HMS gets the newly generated a and nw_u values and sends this data to HES. In addition, it may have some functionalities to detect smart meters acting suspiciously. If it detects a suspicious smart meter, it can inform the accumulator manager to add the suspicious smart meters to the accumulated list to cut off the smart meter from the network (i.e. revoke certificate).

We now describe how the proposed mutual authentication and revocation mechanism work:

- *Revoking Certificates*: Once a certificate is revoked, the CRL collector informs the *Accumulator Manager*.

Accumulator manager performs the computation of the accumulator with the following steps:

  - First, it concatenates the serial number of the revoked certificate and its issuer public key to obtain a unique string. This prevents facing the same serial numbers from different CAs.
  - It calculates a relative prime number in Z_n from the concatenated string. Then, it calculates a new accumulator a_t and ${nw_u}^t$ by adding this prime number to the accumulated list with *NomMemberAdd*. It informs HMS about the new ${nw_u}^t$ and a_t. HMS informs the HES about these values to distribute them to smart meters and gateways.
  - The gateway calculates non-witness values, nw, of each smart meter connected to it using *NonMemWitBatch* and distributes a_t and nw values to the corresponding smart meter.

- *Mutual Authentication and Signing*: The message signing works as in conventional PKI. A smart meter signs its message along with its nw value using its private key and sends it to other party. Obviously, we assume that every component in AMI that has *NonMemberVer* functionality, up-to-date non-witness value nw and latest accumulator value a_t. When authenticating a smart meter, the other party first checks the certificate of smart meter by ensuring the certificate is signed by a trusted CA, it is not expired and the signature is correct. Second, the party uses corresponding nw value to verify that the certificate is still valid by using the *NonMemberVer* function.

Note that with this scheme, there is no need to store and distribute a complete CRL list in smart meters. Instead the smart meters just store an accumulator value and its non-membership witness. Additionally, updating the revocation information will be done with just using a short accumulator value a_t and nw_t. Furthermore, the witness value calculations are done in gateways in a distributed way.This will alleviate the computation cost of the *accumulator manager*, since it will just calculate non-witness update values, nw_u.

V. Performance Evaluation

A. Experimental Setup

The proposed approach is implemented in NS-3 simulator [21] 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 is also implemented in NS-3. We created 4 different grid topologies that consists of 50, 100, 144 and 196 smart meters, respectively. We assumed a transmission range of 120 meters and create grid topologies accordingly. We also prepared a DER (binary) encoded CRL list that has been digitally signed according to RFC 5280 [22] which contains 4500 revoked certificates. We used these certificates and *NonMemWitBatch* function to calculate corresponding accumulator values of each smart meter.

B. Baselines and Performance Metrics

In the simulations, we compared the performance of the proposed approach with two other approaches. In the first approach, we assume that each smart meter keeps the whole CRL locally. In this scenario, we compressed the CRL file and distributed it to smart meters over the gateway. The gateway distributes the CRL by unicasting to the each smart meter. The Constrained Application Protocol (CoAP) [23] was used in unicasting to provide reliability. Note that the CoAP is used with default settings.

In the second approach, a Bloom filter is used to store revoked certificates information. To do so, we read the CRL file and inserted each revoked ID to a Bloom filter by discarding the revocation date information. Bloom filter allows to reduce false positive rates below a certain level by sacrificing its storage advantage [24]. 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 CoAP as in the case of the first approach.

We defined following two metrics to compare the performance.

- *Completion Time*: This metric indicates the total elapsed time to complete the CRL distribution process.
- *Retransmission Count*: This is the total number of retransmissions of CoAP Protocol (i.e., for reliability guarantees) for the same packet at the application layer of the gateway. This metric hints on the communication overhead on the AMI.
- *Storage Overhead*: This indicates the space requirement for the proposed revocation approach.

C. Security Analysis

Our proposed approach addresses all the threats mentioned in Section III. First, through the architectural design in Figure 1 the core of our revocation mechanism (i.e *accumulator manager*) is protected from any attacks by not allowing a direct communication from outside of the network. Second, our accumulator-based approach will not allow verification of a compromised certificate. Moreover, even if the corresponding non-witness value nw of a smart meter is exposed, the authentication will fail while checking the signature of the message. Third, if the gateway is compromised in the same way, its certificate will not be verified by both smart meters and the HES. Fourth, since the HES is in the DMZ area, it has a security provided by firewall. Moreover, HES is the part of the accumulator-based approach and will not communicate with the other parties without verification.

D. Experiment Results

1) Completion Time: : We first conducted experiments to assess the CRL distribution overhead of the proposed approaches.

The results which are shown in Figure 2 indicate that both accumulator and bloom filter significantly reduces required time to finish distribution compared to local CRL approach

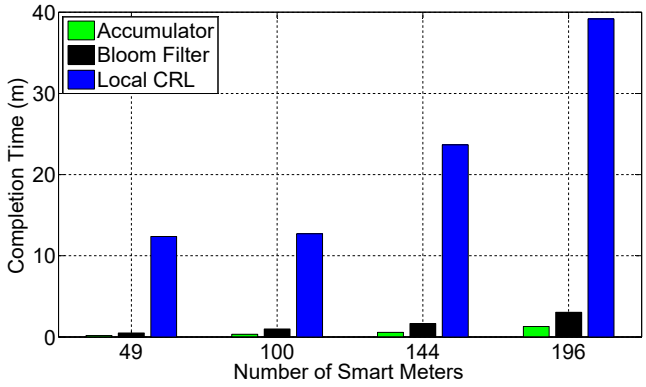

Fig. 2. The completion time of revocation comparison under varying # of meters.

due to condense accumulating. According to these results, the total time for the local CRL approach is increasing at a faster rate than bloom filter and accumulator approach which hints about the scalability of the approaches. Accumulator approach has better scalability when considering the size of the CRL, due to the fact that it is not affected from the CRL size. The accumulator value is independent from the revoked CRL size (the overhead of other methods is proportional to the CRL size) which was 2048 bits in our accumulator settings. This makes accumulator even a better candidate to be employed compared to Bloom filter. For instance in all cases, it reduced the completion time in 3 orders of magnitude compared to Bloom filter approach which is significant.

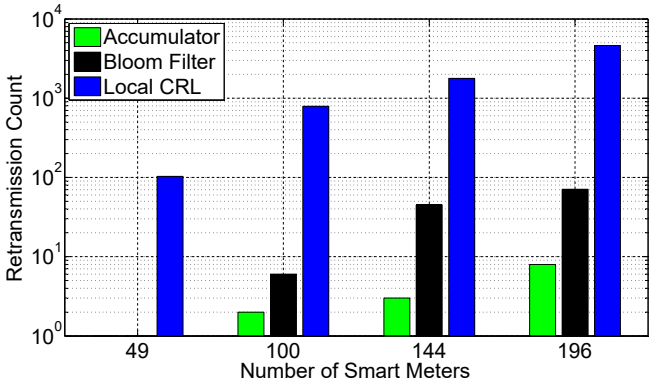

Fig. 3. Retransmission Ratio Comparison under varying # of meters.

2) Communication Overhead: : We compared the performance of the approaches in terms of packet retransmission ratio in order to investigate their overhead. Note that for our scenario, the compressed CRL is sent to a smart meter by using 125 CoAP post messages (i.e., the file fits into 125 messages). Bloom filter needs to send nearly 15 CoAP post messages while accumulator needs to send just one CoAP post message to update the revocation information. Thus, the overhead of our approach is much less in terms of packet count. Figure 3 shows the comparison of these approaches in terms of re-transmission ratio when these post messages are sent. As expected, bloom filter and accumulator have less retransmission count since there will be less traffic congestion to complete the distribution. Again our approach significantly outperforms Bloom filter in reducing the retransmissions. However, for CRL, this is not the case. Due to large number of packets sent, this increases congestion and causes more retransmissions.

3) Storage Overhead: To compare the storage requirements, we identified the needed revocation information size for our approach and compared it with the other approaches, as shown in Table I. As expected, accumulator has a superior advantage since smart meters just needs to store a small accumulator value and non-membership witness value. Local CRL, on the other hand, 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 0.1MB for 4.5K revoked certificates. While Bloom filter's performance is also promising, it is still not better than our approach and it suffers from false positives as discussed before.

TABLE I
CRL STORAGE OVERHEAD

	Local CRL	**Bloom Filter**	**Accumulator**
Required Space (kb)	102.2	6.1	0.7

VI. CONCLUSION

Considering the overhead of certificate and CRL management in AMI networks, in this paper, we proposed a one-way cryptographic accumulator based approach for maintaining and distributing the revocation information in an 802.11s-based AMI. The approach condenses the CRLs into a short accumulator value and builds an efficient and lightweight revocation mechanism in terms of communication overhead. Additionally, non-witness values are calculated in a decentralized manner which helps to alleviate the computation cost of the accumulator manager.

The experiment results indicate that the proposed approach can reduce the distribution and the storage overhead significantly for resource limited smart meters compared to CRL and Bloom filters.

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, pp. 1061–1074, 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, pp. 2742 – 2771, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128612001429

[4] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, 2010.

[5] 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, pp. 937–954, 2007.

[6] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[7] 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, pp. 490–503, 2015.

[8] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer *et al.*, "The matter of heartbleed," in *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014, pp. 475–488.

[9] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas, "The return of coppersmith's attack: Practical factorization of widely used rsa moduli," in *to appear at 24th ACM Conference on Computer and Communications Security (CCS'2017)*. ACM, 2017.

[10] S. Galperin, S. Santesson, M. Myers, A. Malpani, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp," 2013.

[11] Y. Pettersen, "The transport layer security (TLS) multiple certificate status request extension," 2013.

[12] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," in *Crypto*, vol. 2442. Springer, 2002, pp. 61–76.

[13] 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.

[14] 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, pp. 982–988.

[15] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 274–285.

[16] N. Barić and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," in *Advances in CryptologyEUROCRYPT97*. Springer, 1997, pp. 480–494.

[17] J. Li, N. Li, and R. Xue, "Universal accumulators with efficient nonmembership proofs," in *ACNS*, vol. 7. Springer, 2007, pp. 253–269.

[18] L. Reyzin and S. Yakoubov, "Efficient asynchronous accumulators for distributed pki," in *International Conference on Security and Cryptography for Networks*. Springer, 2016, pp. 292–309.

[19] F. Baldimtsi, J. Camenisch, M. Dubovitskaya, A. Lysyanskaya, L. Reyzin, K. Samelin, and S. Yakoubov, "Accumulators with applications to anonymity-preserving revocation." *IACR Cryptology ePrint Archive*, vol. 2017, p. 43, 2017.

[20] M. M. Mahmoud, J. Misic, and X. Shen, "Efficient public-key certificate revocation schemes for smart grid," in *Global Communications Conference (GLOBECOM), 2013 IEEE*. IEEE, 2013, pp. 778–783.

[21] ns 3, "ns-3: network simulator 3," Release 3.24.1, 2016. [Online]. Available: http://www.nsnam.org/

[22] D. Cooper, "Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile," 2008.

[23] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," 2014.

[24] 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, pp. 684–695.