Preserving Consumer Privacy on IEEE 802.11s-based Smart Grid AMI Networks using Data Obfuscation

Andrew Beussink, Kemal Akkaya and Izzet F. Senturk

Department of Computer Science
Southern Illinois University
Carbondale, IL 62901 USA
Email: beussink@siu.edu, kemal—isenturk@cs.siu.edu

Mohamed M. E. A. Mahmoud

Department of Electrical and Computer Engineering
Tennessee Tech University
Cookeville, TN, USA 38505
Email: mmahmoud@tntech.edu

***Abstract*—While the newly envisioned Smart(er) Grid (SG) will result in a more efficient and reliable power grid, its use of fine-grained meter data has widely raised concerns of consumer privacy. In this paper, we propose to implement a data obfuscation approach to preserve consumer privacy and assess its feasibility on large-scale Advanced Metering Infrastructure (AMI) network built upon the new IEEE 802.11s wireless mesh standard. We first propose a secure obfuscation value distribution approach on this 802.11s-based wireless mesh network. Using obfuscation values provided via this approach, the meter readings are obfuscated to protect consumer privacy from eavesdroppers and the utility companies while preserving the utility companies' ability to use the data for state estimation. We assessed the impact of using this privacy approach on the data throughput and delay. Simulation results have shown that the impact of our approach on the network performance is acceptable.**

I. Introduction

The future SG is envisioned as a viable solution for finding efficient and economic methods of addressing a combination of several challenges: 1) using electricity more efficently; 2) reducing the impact of energy production on the environment; 3) integrating renewable energy generated by individuals; 4) building the framework necessary for the use of electrical vehicles [1]. One part of the SG initiative that is currently being implemented is the AMI, which provides two-way communication between the utility company and consumers' "smart" meters (SMs). The utility companies can use this infrastructure to monitor power demands over short periods, provide more accurate billing as well as utilize dynamic pricing to facilitate the reduction of peak demand.

Despite its potential, the implementation of the AMI has aroused concern of consumer privacy, since the fine-grained meter data being collected could be used to infer activities and behavior patterns of consumers [2]. The frequency of the data depends on the application and the premise and can be from 6secs (for businesses) to 15 mins (for residential) as opposed to once a month [1]. This fine-grained data can reveal whether there is someone at home, how many people reside in the house and when they sleep or wake up, etc. This data could commonly be shared with other utility companies and related third parties due to the interconnectedness of the modern power grid. Thus, any effective method of collecting and using fine-grained consumption information from SMs must provide sufficient protection of consumer privacy while preserving the suitability of the data for legitimate uses.

Recently, there has been much research for addressing this privacy issue under different assumptions [3]. While some of the approaches focus solely on the confidentiality of the meter data during its transit, others additionally strive to hide it from utility companies by leaving the handling to trusted third parties. In this way, privacy can be provided by only giving the utility company the chance to do monthly billing and thus no access to individual readings; however, the utility companies then cannot perform state estimation of the power grid, which is crucial to them.

To also accommodate the ability to perform state estimation, a recent study suggested using data obfuscation [4]. This method uses obfuscation to protect consumer privacy of collected fine-grained meter data while preserving the ability of the utility company to monitor the distribution network and calculate billing for given intervals. However, the obfuscation operation necessitates the distribution of obfuscation values to each of the SMs in a secure way which was assumed to be available in that work. In addition, the overhead of this approach on the communication infrastructure at a larger scale has not been investigated. Since the idea is promising, it is important to investigate its performance when it is implemented and fully applied in an AMI network.

In this paper, we propose to employ this technique in a large-scale network, namely an 802.11s-based wireless mesh network. This is envisioned to be one of the underlying communication architecture for AMI applications [1][5]. We propose an approach for distribution of obfuscation values in an efficient and secure manner based on the security goals identified. We then implement this distribution approach and simulate obfuscated data traffic on ns-3 by using a draft version of the 802.11s implementation. Our goal is also to assess the

978-1-4799-3088-3/14/$31.00 ©2014 IEEE

overhead it brings to the network and compare the overhead to that of a regular 802.11s network which does not provide privacy preservation.

The simulation results revealed that such use of obfuscation brings only slight overhead in terms of delay compared to the case when no privacy/security is provided while it maintains the same throughput. With the ability to perform state estimation and providing consumer privacy, the approach is feasible to be used in 802.11s-based AMI networks with large scales.

The rest of the paper is organized as follows. In the next section, we provide a summary of the related work. In section III, we provide some background on state estimation in power grids. Section IV describes the assumptions, security goals and problem. In Section V, we present our approach for obfuscation value distribution in a secure manner. Section VI includes the discussion on the achievement of security goals. Section VII is dedicated to experiment results. Finally, we conclude the paper in Section VIII.

II. Related Work

In general, the utility companies need fine-grained meter data for each customer to monitor demand and the state of the network as well as utilizing dynamic pricing to reduce peak demand. Also, the utility companies would prefer to have the data to generate the bill on-site rather than relying on each individual SM. Thus, the SG should allow the utility companies to collect and use this fine-grained data while protecting it from being used to monitor or profile an individual consumer's behavior.

Various approaches of providing consumer privacy are surveyed in [3]. This work categorizes these approaches into three groups, approaches that anonymize the fine-grained meter data, approaches that mask or obfuscate the individual consumption, and approaches that focus only on protecting communication of meter data from threats in the communication network. In practice, the third category does not provide any additional mechanism for ensuring privacy other than relying on the trustworthiness of the utility companies.

Two approaches can satisfy the aforementioned requirements: anonymizing the data by using an escrow service [6] and masking usage patterns by using an internal power supply to shape the actual consumption data [7]. Masking usage patterns with an internal power supply enables the utility company to collect the actual data without posing a privacy risk. It can also help reduce peak demand by having the power supply provide power during peak time and recharge when demand is low. However, the cost of implementation and maintenance of these systems make it less than ideal to both the utility company and the consumer.

The approach using an escrow service creates two identities for each customer, one for the SM to use for communication related to billing purposes and another for the collection of fine-grained meter data [6]. This approach is not sufficient, since it requires the escrow service to be trustworthy about the actual identities. This could then be circumvented by capturing both types of data and inferring the relationship between an individual SM's two identities. Since the utility company possesses the actual fine-grained meter data, it would then be able to determine the behavior of individual customers.

Our privacy approach in this paper is based on obfuscation [4]. To the best of our knowledge, the obfuscation approach in [4] is the only approach in the literature that protects consumer privacy while allowing the utility company to perform state estimation and billing and dynamic pricing. Our work makes contributions different than this work in two ways: First, there was no distribution mechanism of obfuscation values in that work since no underlying NAN was mentioned for AMI. We propose using an IEEE 802.11s-based mesh networking for the implementation of NAN. Second, we present a secure way of distributing the obfuscation values in such a network. Finally, we assess the overhead of obfuscation value distribution in this mesh network.

III. Background

A. Weighted Least Squares State Estimation

A power system consists of a collection of buses, transmission lines and power meters. State estimation is used to monitor the state of a power system (i.e., voltage and phase of every bus) in order to maintain reliable power transmission. One of the techniques for this process is called common weighted least squares (WLS) state estimation.

In this technique, the state of the network is estimated as a vector $x = (x_1, \ldots, x_n)^T$ using $z = (z_1, \ldots, z_m)^T$ consisting of measurements from the power meters where n, m are positive integers such that $m > n$ and $x \in \mathbb{R}^n$ and $z \in \mathbb{R}^m$. Then, the state of the system is represented by:

$$z = h(x) + e$$

where $h : \mathbb{R}^m \rightarrow \mathbb{R}^n$ represents nonlinear dynamics such as the configuration of transformers and buses in the grid and $e \in \mathbb{R}^m$ is measurement errors and unmodeled dynamics. The state x is estimated to be $\hat{x}$ by the following unbiased linear estimation:

$$\hat{x} = (H^T W H)^{-1} H^T W z$$

where W^{-1} is the covariance matrix of e.

B. Privacy-Preserving State Estimation

The authors in [4] create a *distortion free obfuscation space* from the span of a basis set $\mathbb{O} = \{o_1, \ldots, o_{m-n}\}$ of *kernel* denoted as $ker((H^T W H)^{-1} H^T W)$. They create an *obfuscated measurement vector* named z_{obf} where $z_{obf} = z + o, o \in \mathbb{O}$. They show that z_{obf} can be used in place of z to calculate the same estimated state $\hat{x}$. In this way, without having access to actual power readings, the state of the power grid can be estimated.

Specifically, their approach assumes a lead meter (LM) in the grid which receives the basis set $\mathbb{O}$ from the utility company. $\mathbb{O}$ is derived from the state of distribution of the grid such as the configuration of the transformers stepping up or down voltages or buses branching off to multiple distribution lines. It can be sent by the utility company only when

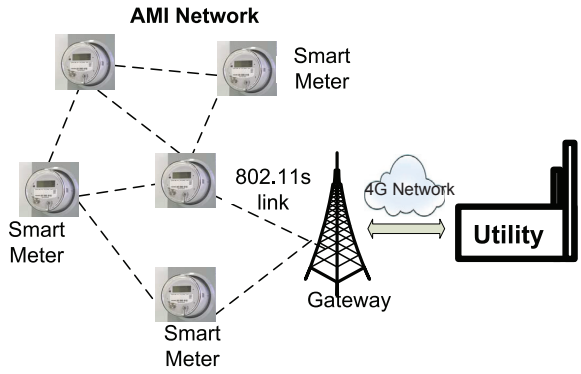

Fig. 1: A sample AMI communication network, gateway and long-distance communication to utility company.

something changes. It can be reused for multiple readings until new ones are provided.

The LM randomly generates the values η to create an obfuscation vector o. At measurement time t_j, the goal is to choose a random weight $\eta_i^j \in \mathbb{R}$ for a vector $o_i \in span(\mathbb{O}) = \{\eta_1^j o_1, \ldots, \eta_{m-n}^j o_{m-n}\}$. The values of the weights η_i^j at each data collection time t_j, in a billing period T are chosen so that the sum of the values of η_i^j in T sum to 0 (i.e.,$\sum_{j \in T} \eta_i^j = 0$).

After the above computation is done, an element from the vector o is sent to the corresponding SM. Each SM adds this element to its actual power measurement and sends it to a third-party computing service. The computing service then constructs the obfuscated measurement vector z_{obf} and calculates the billing information for that billing period. This information is sent to the utility company which uses this information to perform state estimation and calculate billing. All communications are assumed to be over secure channels.

IV. Preliminaries

A. Assumptions

We assume that the AMI communication network consists of SMs that are connected via a wireless mesh network with one gateway serving as a relay between the SMs and the utility company as shown in Fig. 1. The mesh network is created using the new IEEE 802.11s standard which allows mesh networking among the SMs through 802.11 MAC/PHY layer standard [8]. In this mesh network, the gateway collects meter readings that are obfuscated at the SMs via multi-hop routes. The gateway is also responsible for providing obfuscation information to the SMs. We assume that the gateway communicates with the utility company via a long distance communication (e.g., 4G, WiMax).

Each SM is initialized with a public/private key. The gateway possesses the public key of every SM in its mesh network. Every SM possesses the public key of the gateway. We assume that the gateway and SMs are tamper-resistant and cannot be compromised.

B. Problem Definition

Our problem can be defined as follows: "Given an 802.11s-based wireless mesh network with a gateway, our primary goal is to distribute the obfuscation values to the SMs and collect the obfuscated values from them securely and privately without requiring any third party service providers. Our secondary goal is to assess the overhead of this process in a large scale AMI network and thus analyze the feasibility of the approach for future SG applications." The security goals are elaborated next along with the corresponding attacks. Note that these security goals are in addition to the goals of preventing misuse of finely-grained meter data and preserving the ability to perform state estimation.

C. Threat Model and Security Goals

We identified the following attacks to the privacy and security of the collection of fine-grained meter data in the AMI and established the associated security goals. They are organized into two sets, those targeting the consumer and those targeting the utility company. The first set relates to the privacy of a consumer's fine-grained meter data.

- *Attack 1*: The utility company misuses fine-grained meter data it obtains to analyze consumer behavior or shares the data with a third party for this purpose.
- *Security Goal 1*: Obfuscate the collected fine-grained meter data to protect it from misuse by the utility company or related third party.
- *Attack 2*: An eavesdropper monitors the communication channel to capture meter data in messages between a targeted SM and the gateway to determine the behavior of its consumer.
- *Security Goal 2*: Protect communications containing SM readings.

The second set of attacks relates to accurate state estimation and billing.

- *Attack 3*: An attacker impersonates the gateway and sends fabricated obfuscation values to the SMs to change the state of the power network.
- *Security Goal 3*: Provide sender authentication to verify the sender and contents of messages.
- *Attack 4*: An attacker captures the obfuscation values and replay them to change the state or billing.
- *Security Goal 4*: Prevent the replay of messages.

V. Data Obfuscation on a Wireless Mesh Network

A. Overview

In this section, we describe in detail the design of a realistic architecture and procedures for obfuscating and collecting SM data. The approach has two phases: First, obfuscation values are created and distributed in the mesh network. Second, each SM creates its obfuscated power reading and transmits it to the gateway. To provide privacy and security, our network architecture makes use of elliptic curve cryptography (ECC). This was chosen since its overhead is the minimal in comparison to other public cryptography techniques. The choice

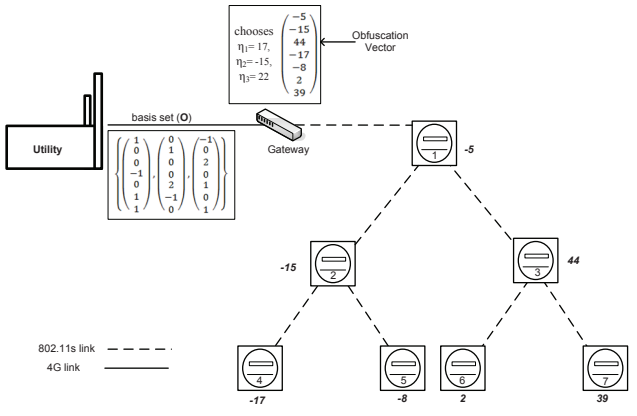

Fig. 2: A mesh topology of 7 SMs. First, the gateway receives the obfuscation basis from the utility provider and creates the obfuscation vector by picking random η values and multiplying them with each vector of the $\mathbb{O}$. Then, each obfuscation element (italic) (i.e., $o[j]$ where j : 1 to 7) is communicated to its corresponding SM.

of an asymmetric technique is mainly its convenience with key management compared to symmetric techniques. Provision of non-repudiation is also a plus which does not exist in symmetric-key systems. ECC also uses a key size comparable to current symmetric cryptographic schemes, avoiding the higher computation of other public key schemes due to the larger key size. Note that our approach avoids the assumption that each SM has a communication link with the third-party computation service. The obfuscated readings are collected in-network and communicated to the utility company.

B. Creating the Obfuscation Vector

The gateway is responsible for creating the obfuscation vector. To do this, the utility company first sends the basis of the obfuscation space, $\mathbb{O}$, to the gateway. The gateway then randomly selects weights (η) for each of the vectors in the basis and constructs an obfuscation vector. An example for a simple mesh topology is provided in Fig. 2. In this example, upon receiving $\mathbb{O}$, the gateway randomly chooses weights for each vector o_i in $\mathbb{O}$ and constructs the actual obfuscation vector o.

Let a sample $\mathbb{O}$ be:

$$\{(1,0,0,-1,0,1,1)^T, \\ (0,1,0,0,2,-1,0)^T, \\ (-1,0,2,0,1,0,1)^T\}$$

and the gateway randomly generates the weights $\eta_1 = 17, \eta_2 = -15, \eta_3 = 22$ at time t_1. It then constructs the obfuscation vector o as follows:

$$17 \times (1,0,0,-1,0,1,1)^T \\ + (-15) \times (0,1,0,0,2,-1,0)^T \\ + 22 \times (-1,0,2,0,1,0,1)^T \\ = (-5,-15,44,-17,-8,2,39)^T.$$

Note that the gateway stores a sum of (η) values for each obfuscation vector o during a particular billing period (e.g., $T = \sum_{j=1}^{j=n} t_j$): $sum = \sum_{t_j=1}^{t_j=n} \eta_i^j$ where i can get values from 1 to the number of vectors in $\mathbb{O}$. When the final meter reading for a billing period is collected, the gateway chooses the weight (η_i^n,) for a particular obfuscation vector o so that the sum becomes zero. Thus, η_i^n is chosen as $-\sum_{t_j=1}^{t_j=n-1} \eta_i^j$ so that $\sum_{j=1}^{j=n} \eta_i^j = 0$. For the example in Fig. 2, if we assume that there are two more collection times, t_2 and t_3, using the same $\mathbb{O}$, the weights can be as follows: At t_2, let us assume that the weights are again randomly chosen as 10, 12, 3. At t_3, the weights must be chosen as -27, 3, -25 so that the $\forall i$: $\sum_{j=1}^{j=3} \eta_i^j = 0$.

C. Secure Distribution of Obfuscated Values from Gateway

Once the obfuscation vector o is created at the gateway, it encrypts the elements in the vector with the public key (PU_i) of its corresponding SM_i. The gateway then sends each SM its corresponding element of the obfuscation vector separately by signing it with its private key PR_G as follows. This is also illustrated in Fig. 2:

$$Gateway \rightarrow SM_i : \{\eta_i\}_{PU_i}, \{\{\eta_i\}_{PU_i}\}_{PR_G}$$

D. Calculating & Transmitting Obfuscated Measurements

When an SM_i receives its element from the obfuscation vector, say $o[i]$[1], it calculates its obfuscated power measurement (op_i) by taking its current power reading (p_i) and adding it to $o[i]$: $op_i = p_i + o[i]$. It then timestamps (TS) the sum and digitally signs the message for gateway using its private key, PR_i. The SM then transmits this to the gateway using 802.11s routing:

$$SM_i \rightarrow Gateway :< TS, op_i >, \{< TS, op_i >\}_{PR_i}$$

Upon receiving the obfuscated measurements from each SM, the gateway verifies the digital signatures and timestamps. It then sends them to the utility company. The utility company can then use the obfuscated measurement vector for state estimation. In addition, once it receives all of the obfuscated measurements for the current billing period, it can sum them to receive the actual usage for each SM for the billing period to charge the customer. Based on the $\mathbb{O}$ in Fig. 2, the calculation and collection of the measurements are depicted in Fig. 3.

VI. Security Analysis

In this section, we evaluate our proposed approach based on the security goals listed in Section IV-C.

- *Security Goal 1*: Since the fine-grained meter data is obfuscated, the actual reading cannot be determined at any time. Because of this, it cannot be analyzed to determine any activity or behavior of the consumer.
- *Security Goal 2*: The obfuscated reading that the SM sends to the gateway does not reflect the actual reading.

[1]Note that we use o_i to refer to a vector while $o[i]$ is referring to a particular element in a vector.

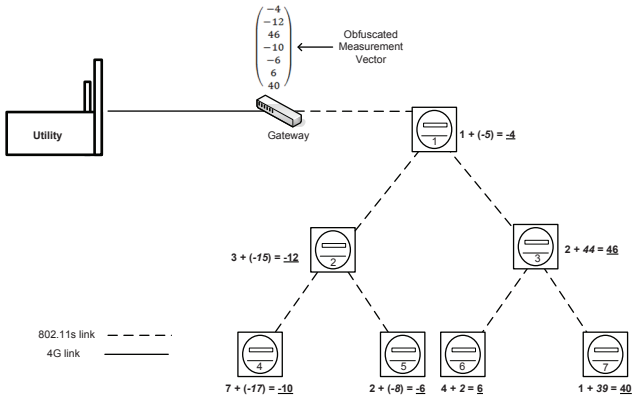

Fig. 3: Each meter adds its current reading to the received obfuscation values to calculate its obfuscated reading (underlined). SM_4, for example, has a current reading of 7. It sums it with the obfuscation value it received, -17, obtaining an obfuscated reading of -10. The obfuscated readings are securely communicated back to the gateway which constructs the obfuscated measurement vector, z_{obf}. This is sent to the utility company.

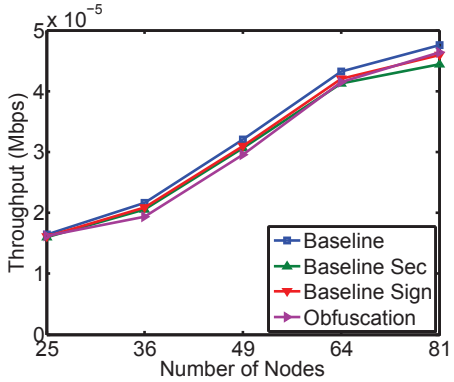

Fig. 4: Throughput for varying number of nodes.

Therefore, even if an eavesdropper captures this reading, its inference about the activity in the house will be wrong.

- *Security Goal 3*: Since all of the SMs use digital signatures for messages containing obfuscation information and measurements, the digital signature can be verified to confirm the identity of the message sender. In addition, since the messages are digitally signed, they cannot be modified without invalidating the digital signature, providing message integrity.
- *Security Goal 4*: Since all messages are timestamped and digitally signed, the timestamp can be checked to verify that the received message is for the current reading.

VII. Experimental Evaluation

A. Experiment Setup

We implemented the proposed approach in ns-3 [9], which contains a draft version of IEEE 802.11s. Random connected AMI network topologies were created containing 25, 36, 49, 64 and 81 nodes in an area of size 1200mx1200m. Note that the area mimics the size of a neighborhood which will be using a single gateway to communicate with the utility company. The transmission range of each node is 100m. The gateway is also picked randomly and thus can be located anywhere in the network. The underlying MAC for each SM is IEEE 802.11g. TCP is used to ensure reliability compared to UDP. The data frequency for the SMs is set to 10sec. to accomodate any stress testing to the network in case it is used to collect data for industrial offices where the data collection frequency is as low as 6secs. The simulation is run for 1000secs. We tested each run for 30 different topologies which are created randomly and reported the average of these topologies for significance of the results.

For encryption, we used crypto++ library [10]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is an approved signature algorithm for the US government use [11] and the Elliptic Curve Integrated Encryption Scheme (ECIES) is a well-known scheme having several standards [12]. ECDSA is used when only signature is required and ECIES is used when encryption and signature are required. In both cases, we used the ASN.1 secp128r1 standard curve with SHA1, having a key length of 256 bits.

B. Baselines and Performance Metrics

We considered three baselines for comparison with our approach. The first baseline (represented as "baseline" in the graphs) sends meter readings in the clear, providing no privacy. The second baseline (represented as "baseline sign") provides authentication but does not provide any confidentiality in transmission and the utility provider has access to the fine-grained meter data. The third baseline (represented as "baseline sec" in the graphs) provides authentication as well as confidentiality in transit, but the utility provider still has access to the fine-grained meter data.

In analyzing the results, we considered two metrics: throughput (i.e., the amount of data received at the gateway per second) and data delay (i.e., the total time it takes for a reading to reach the gateway).

C. Simulation Results

1) Throughput: The results of the experiments conducted for assessing the throughput are shown in Fig. 4. The throughput for the baselines and the proposed approach is similar. The throughput increases as the network size grows due to the contribution of more nodes as expected. We observe that without using any encryption or authentication, the throughput is slightly larger due to non-existence of the data overhead in the packets. Note that we perform encryption or authentication at the application layer. Therefore, the performance at the TCP layer does not change. However, the carried data size is slightly reduced which results in a slightly better performance for the baseline.

In the case of our approach, there seems to be a very slight decrease in the throughput as in the cases of encryption or authentication. We believe that this is caused due to the crossing of traffic when the obfuscation values are being sent

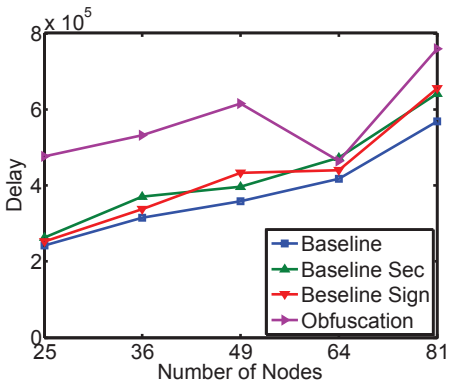

Fig. 5: Average end-to-end delay for varying number of nodes.

from the gateway to the SMs and a short time after the readings are being sent from SMs to the gateway through the same paths. While these transmissions are happening one after another, there may still be some traffic in the network during the transmission of obfuscation values to the leaves (i.e., the nodes at the far end of the network) of the network topology. This can cause some interference and keep the channel busy at certain parts of the network which eventually causes the throughput to reduce slightly. However, overall these results indicate that there is no major adverse effect of the proposed distribution and obfuscation approach in terms of throughput.

2) End-to-end Delay: We also looked at the impact of the approach on end-to-end delay, an important metric for some of the AMI applications such as demand response. The results are shown in Fig. 5. The delay for the proposed approach is greater than the other baselines when the network size is smaller (i.e., up to 49 nodes). This can be explained as follows: Our approach has the phase of sending obfuscation values to the SMs. The SMs wait for these values to send their readings. This waiting adds to the end-to-end delay of the readings when compared to other approaches which do not need to wait for any messages to arrive. However, the contribution of this overhead disappears when the network size grows. We speculate that this happens because of the following reason: Since the SMs are waiting for obfuscation values, they cannot send their readings around the same time. The obfuscation values reach the destinations at different times due to the topological structure of the network. Since the SMs send at different times, this reduces the contention among the nodes for accessing the channel in the network and thus MAC layer delay is reduced. Eventually, the additive path delay is reduced compared to other approaches. Note that in the other approaches, more nodes become involved in message sending and thus channel access delay increases significantly due to heavy contention and interference. Considering the fact that the mesh network size is much larger in AMI networks, our approach amortizes the impact of obfuscation distribution, making it feasible for practical cases.

VIII. Conclusion

In this paper, we implemented a data obfuscation approach for a 802.11s-based mesh network to assess its overhead. We proposed mechanisms to securely distribute obfuscation values. The values are sent using the routes available via 802.11s. We analyzed the approach in terms of the security goals it provides and showed that it can ensure consumer privacy while still allowing state estimation and billing. The implemented approach under ns-3 using a draft version of 802.11s showed that while there is slight waiting delay when the network size is smaller, such delay overhead does not exist as the network size grows. In addition, the throughput of the proposed approach is comparable to the baselines which makes the approach feasible for large-scale AMI applications.

IX. Acknowledgement

This work is supported by US National Science Foundation under the grant number 1318872.

References

[1] W. Wang, Y. Xu, and M. Khanna, "Survey paper: A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, pp. 3604–3629, October 2011. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2011.07.010

[2] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proceedings of the 11th international conference on Privacy enhancing technologies*, ser. PETS'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 175–191. [Online]. Available: http://dl.acm.org/citation.cfm?id=2032162.2032172

[3] N. Saputro and K. Akkaya, "On preserving user privacy in smart grid advanced metering infrastructure applications," *Security and Communications Networks*, to appear.

[4] Y. Kim, E.-H. Ngai, and M. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, oct. 2011, pp. 178 –183.

[5] 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

[6] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 238 –243.

[7] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, oct. 2010, pp. 232 –237.

[8] The status of ieee 802.11s standard. [Online]. Available: http://grouper.ieee.org/groups/802/11/Reports/tgsupdate.htm

[9] "Network simulator - ns - 3," *http://www.isi.edu/nsnam/ns/index.html*.

[10] "cryptopp," *http://www.cryptopp.com/*.

[11] NIST, "Fips 186-3: Digital signature standard," 2009.

[12] V. Gayoso Martnez, L. Hernndez Encinas, and C. Snchez vila, "A survey of the elliptic curve integrated encryption scheme," *Journal of Computer Science and Engineering*, vol. 2, no. 2, 2010.