Secure Information Aggregation for Smart Grids Using Homomorphic Encryption

Fengjun Li
College of IST
The Pennsylvania State University
University Park, PA, 16802
Email: fli@ist.psu.edu

Bo Luo
Department of EECS
The University of Kansas
Lawrence, KS, 66045
Email: bluo@ku.edu

Peng Liu
College of IST
The Pennsylvania State University
University Park, PA, 16802
Email: pliu@ist.psu.edu

***Abstract*—In this paper, we present a distributed incremental data aggregation approach, in which data aggregation is performed at *all* smart meters involved in routing the data from the source meter to the collector unit. With a carefully constructed aggregation tree, the aggregation route covers the entire local neighborhood or any arbitrary set of designated nodes with minimum overhead. To protect user privacy, homomorphic encryption is used to secure the data en route. Therefore, all the meters participate in the aggregation, without seeing any intermediate or final result. In this way, our approach supports efficient data aggregation in smart grids, while fully protecting user privacy. This approach is especially suitable for smart grids with repetitive routine data aggregation tasks.**

I. Introduction

Smart grids are envisioned by numerous and diverse stakeholders as the next-generation approach of delivering electricity to millions of households worldwide [1]–[6]. The smart grids have introduced computation and communication capabilities into traditional power grids to make them "smart" and "connected". Processing chips and storage units have been embedded into traditional electricity meters, so that they are capable of performing "smart" functions. Then, smart meters communicate with electrical appliances at home as well as the generation and management facilities at the power companies, providing smart grids with great connectivity. Research and implementation on smart grids could be categorized at three layers [7]: "*smart generation, smart grid, and smart customer*." With the intelligent and networked meters, the smart grids enable instant monitoring of power delivery and consumption information, subscription of power usage and controlling from remote, advanced demand and outage management, usage management especially with respect to pricing (e.g. charging electrical cars at none-peak hours), etc. Therefore, it benefits end-users as well as power generation and distribution. Moreover, smart electricity meters could be further linked with smart water and gas meters to better coordinate and manage energy usage for smarter/greener homes [8].

However, with all the advantages introduced by smart grids, security and privacy concerns start to arise [9], [10]: 1. hackers could compromise smart meters to manipulate power usage and energy costs. 2. Cyber-terrorists might fake power consumption data at a large scale to attack the power system, e.g. overloading nuclear power plants. 3. Attackers hacking into others' smart meters may control and tease with their electrical devices. 4. Adversaries might compromise smart meters, eavesdrop the communication, or hack into power company's database, to access power consumption data of the victim, from which they learn about the victim's daily activities, habits, and other privacy with reasonable inferences. Many security and privacy vulnerabilities and threats have been studied in the research literature, however, most of the problems remain unanswered.

Instant aggregation of data and resources is an important function in smart grids [11]. For instance, aggregations of power usage data at multiple levels (neighborhood, subdivision, district, city etc) are conducted at different frequencies. Such information is essential for monitoring and predicting power consumption, allocating and balancing loads and resources, and administering power generation, etc. Therefore, it is of great importance to provide *efficient* and *secure* data aggregation in smart grids. To tackle the challenge, we present in-network aggregation for smart grids, in which aggregation is performed in a distributed manner, instead of centralizing at the collector devices. To protect user and neighborhood privacy in the aggregation, we employ homomorphic encryption to ensure that intermediate results are not revealed to any device en route, while still maintaining an efficient and effective aggregation process.

The rest of the paper is organized as follows: in Sections 2 and 3, we introduce related works and background, especially homomorphic encryption. In Section 4, we present our problem and explore possible solutions. We conclude the paper in Section 5.

II. Related Works

Research on smart grid spans a wide spectrum: from technology [12]–[14] to economy, marketing, policy and legal issues [15], [16]; from power generation, transmission, distribution [17], [18], to load management, failure diagnosis and recovery [19]–[21], to smart meter implementation and communications [13], [22]–[25]. Among these topics, we are particularly interested in security and privacy of smart grids. [9] identifies several security and privacy vulnerabilities/threats in smart grids, and calls for attention and efforts

978-1-4244-6511-8/10/$26.00 ©2010 IEEE

from government, academia and industry. [10] reviews the security challenges in smart grids, with a special focus on trust, authentication and encryption. In [26], [27], Metke and Ekl have articulated the security requirements for smart grid networks, and pointed out different security technologies to fulfill such requirements. Particularly, they have elaborated public key infrastructure (PKI) and trustworthy computing, and the potential adoption in smart grid networks. As a comparison, we focus on a particular problem - secure information aggregation in smart grids, instead of covering the broad area.

Various in-network data aggregation approaches have been proposed for sensor networks (e.g. [28], [29]), in which sensors are extremely restricted in computation and communication power due to their limited battery. In smart grid systems, although power of the smart meters is usually not a concern, communication bandwidth may still be insufficient, especially when frequent aggregation is desired. Meanwhile, sensors in the network are usually trusted to see the data from other sensors and the intermediate aggregation results, and most secure aggregation researches focus on defending against passive attacks (e.g. eavesdropper) [30], [31] or the attacks tampering with the aggregation mechanism using fake inputs [32], [33]. However, in smart grids, power usage is considered as privacy of the owner, and should not be revealed to other meters. Therefore, traditional tree-based aggregation on plaintext does not apply. In this paper, we employ homomorphic encryption to perform in-network aggregation but still keep the outputs and intermediate results secure.

III. Background

A. Homomorphic Encryption

Homomorphic encryption represents a group of semantically secure encryption functions that allow certain algebraic operations on the plaintext to be performed directly on the ciphertext. Mathematically, given a homomorphic encryption function $\mathsf{E}()$, and two messages $x, y \in \mathbb{Z}_N$, we are able to compute $\mathsf{E}_k(x \star y) = \mathsf{E}_{k_1}(x) \circ \mathsf{E}_{k_2}(y)$, without knowing the plaintext x, y or the private key. In practice, $\star$ represents addition or multiplication operations. Homomorphic encryption is usually used for privacy-preserving operations (e.g. voting), in which operations are performed but operands (inputs) are not disclosed. Well-known homomorphic encryption schemes include: RSA, El Gamal [34], Paillier [35], Naccache-Stern [36], Boneh-Goh-Nissim [37], etc. In this work, *additive homomorphic* property is desirable for in-network data aggregation, therefore, we adopt Paillier cryptosystem [35], [38]. It is one of the two commonly used additive homomorphic encryption functions, while the other one – the Boneh-Goh-Nissim (BGN) cryptosystem [37] – is an extension of Paillier with bilinear groups. The Paillier cryptosystem works as follows:

Key Generation

1) Pick two large prime numbers p and q;
2) $N = p \cdot q$ and $\lambda = \mathrm{lcm}(p-1, q-1)$, where lcm represents least common multiple.
3) Select a random number g where $g \in \mathbb{Z}^*_{n^2}$.
4) Set function $L(u)$ as: $L(u) = (u-1)/N$.
5) Ensure that N divides the order of g: check if $L(g^\lambda \mod N^2)$ and n are co-prime, i.e. $\gcd(L(g^\lambda \mod N^2), N) = 1$.
6) (N, g) is the public key.
7) (p, q) is the private key.

Encryption

1) We want to encrypt the message: $m \in \mathbb{Z}_N$.
2) Select a random number: $r \in \mathbb{Z}^*_N$.
3) Encrypt m using: $c = \mathsf{E}(m) = g^m \cdot r^N \mod N^2$

Decryption

1) We want to decrypt ciphertext: $c \in \mathbb{Z}^*_{N^2}$
2) Decrypt with: $m = \mathsf{D}(c) = (\frac{L(c^\lambda \mod N^2)}{L(g^\lambda \mod N^2)}) \mod N$

Given $c_1 = \mathsf{E}(m_1)$ and $c_2 = \mathsf{E}(m_2)$, $\forall m_1, m_2 \in \mathbb{Z}_N$, we have $\mathsf{D}(c_1 \cdot c_2 \mod N^2) = m_1 + m_2 \mod N$ – the sum of plaintext is calculated from multiplication of the ciphertext. Also, Paillier cryptosystem is indeterministic (i.e. the same message will be encrypted into difference ciphers using different random blinding factor r), which makes it resistant to dictionary attacks.

B. Honest-but-curious Model

In this paper, we assume all participants follow the honest-but-curious adversary model, a.k.a. semi-honest model [39]. In this model, all parties are assumed to follow the protocol properly ("honest"); meanwhile, they keep all inputs from other parties and all intermediate computation results, from which they actively seek or infer knowledge about others ("curious"). Therefore, honest-but-curious adversaries keep the system functioning properly to avoid being identified by intrusion/abnormal detection mechanisms, while maximizing the chance of obtaining others' privacy.

In our scenario, honest-but-curious smart meters do not tamper with the aggregation protocols: they do not spitefully drop or distort any source value or intermediate result; and they keep the system running smoothly. However, they will try to infer others' electricity usage by analyzing messages and values that have been routed through them.

IV. Secure Information Aggregation

A. Problem and solution overview

Although there have been different proposals on the smart grid communication infrastructure, the wireless-wired multi-layer architecture is the most popular approach, and has been adopted in some pilot projects. In this architecture, smart meters in the neighborhood communicate with a *collector device* through a wireless mesh network. The collector device further communicates with the central management facility through wired communication (LAN or dial-up) [9], [13], [14]. Figure 1 shows an example of the communication infrastructure for a neighborhood with 20 homes.

Data aggregation (e.g. average power usage of the neighborhood) is a very important type of query in smart grids [11]. Traditionally, each smart meter establishes a connection with the collector, and uses it exclusively to report its data to

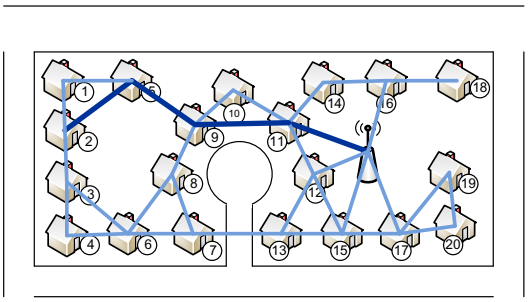

Fig. 1. An example of smart grid communication in a neighborhood.

the collector. The collector handles all the simultaneous connections, calculates the aggregation results, and reports it to the central management. Although it is simple and easily adoptable, this approach introduces excessive network traffic, as well as overwhelming demands at the collectors.

Example 1 *If we look at the example shown in Figure 1, connection between meter 2 and the collector is routed through meters 5, 9, 11, etc. For an aggregation query that covers the entire neighborhood, it simultaneously establishes 20 such connections, most of which are redundant.*

Therefore, we propose an in-network incremental aggregation approach – instead of requiring each meter to create an independent connection with the collector, we ask enroute meters to share the channel. The first step of our approach is to construct a virtual aggregation tree based on the network topology of the wireless mesh. In a bottom-up aggregation, each node in the tree collects data from its children, computes an aggregation of all such data and its own, and passes the aggregated result to its parent. The collector, as the root node, ultimately gets the aggregation over the entire tree. At a broader scope, we define *in-network operations for smart grids* as follows:

Definition 1 (in-network operations for smart grids) *An operation at the collector device takes input from all (or a subset of) N smart meters: $I_1 \star I_2 \star ... \star I_i \star I_N$, where $\star$ is the operation, and I_i is the input from smart meter i. If the operation is associative and commutative, we are able to perform the operation of $\star$ in any arbitrary order, and deploy some of the computation to the smart meters in the network.*

Use data aggregation operation in smart grids as an example. The $\star$ operation could be *sum* (e.g. total utility usage in a neighborhood) or *count* (e.g. number of homes in the neighborhood that are using a certain device).

In traditional aggregation approach, each participating smart meter sees intermediate aggregation results routed through itself. Even though link encryption is often applied to protect messages from being recovered by eavesdroppers, intermediate smart meters are allowed to decrypt the collected data, considering mathematical operations for aggregation tasks cannot be performed over commonly encrypted ciphertext. However, this will introduce a serious privacy issue, since it is commonly acknowledged that utility usage information carries a significant amount of user privacy.

To tackle the privacy issue introduced by plain-text aggregation, we employ homomorphic encryption to enable both secure in-network aggregation and privacy protection: electricity usage data from child smart meters are encrypted with a semantically secure encryption scheme; meanwhile, algebraic operations of the plaintext are allowed to be performed on the cipher domain to enable aggregation functions (e.g. sum and count), with a reasonable computation overhead.

B. The Aggregation Tree

To enable in-network aggregation, we need to first construct an aggregation path, which covers all the smart meters in the neighborhood. For each aggregation task, all or a subset of the nodes on the aggregation path are selected to participate in the task.

If we consider the smart meter network as a graph $G(V, E)$, where V is the set of smart meters (as vertices) and E is the set of available wireless links (as edges) between any two smart meters. Intuitively, the aggregation tree is a *spanning tree* of the graph, which consists of a (minimal) subset of E that connects all vertices in a hierarchical structure. In order to include all the vertices in the tree, the graph should be connected – every smart meter should have at least one communication path to the collector device. For a given graph, there may exist multiple spanning trees of different structures.

An aggregation tree should always root at the collector node, which initializes all the aggregation tasks and collects the final results. Meanwhile, for a network with N smart meters (excluding the collector device), every aggregation tree will consist of $N + 1$ nodes and N edges. The aggregation is recursively calculated in a bottom-up manner: every node in the aggregation tree takes inputs from itself and its children nodes; it then aggregates the data and sends the result to its parent node.

There are two major concerns on constructing the aggregation tree: (1) the height of the tree should be small, to reduce the maximum hops for the longest aggregation path, thereby reduces end-to-end aggregation time; (2) an interior node of the tree should not have too many children, to avoid excessive computation and communication load at the node.

To achieve the first goal, the spanning tree is constructed by a breadth-first traversal of the graph, starting at the collector node. In this way, the height of the tree is the same as the shortest distance from the furthest node to the collector – the tree is shallow but wide. In the case that a node K has too many children, it may possibly become a bottleneck in the aggregation. In such cases, we *re-balance* the tree: we first check if a child of K is also connected to a less-populated sibling of K, and then move the child to that sibling; if K still has too many children, we check if a child is also connected to another child of K, and move it to that child. Note that the first action will not increase the height of the tree, while the second one may do so.

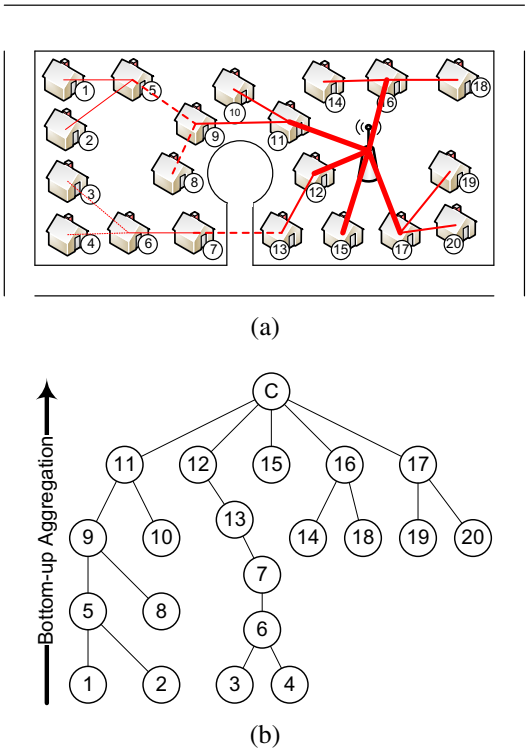

Fig. 2. An example of aggregation tree construction: (a) breadth-first traversal of the network graph; (b) the aggregation tree constructed from the traversal.

The network routing in the smart meter network is relatively static. In most cases, the collector device has the network graph of the entire neighborhood. Therefore, the aggregation tree is constructed locally at the collector, without probing all the smart meters. In addition, an aggregation graph remains stable for an extended period of time.

Example 2 *Figure 2(a) shows an example of the breadth-first traversal of the graph shown in Figure 1, while Figure 2(b) shows the resulting aggregation tree. Assume the collector is not able to handle five children simultaneously, we re-balance the tree by moving node 15 to node 12.*

C. In-network aggregation using homomorphic encryption

With the aggregation tree, we construct operation plans for participating nodes, and deploy them to the smart meters in a top-down manner. Particularly, an operation plan for a smart meter is a 7-tuple: $\{T_{ID}, Trigger, Data, Collect, Operation, Destination, Key\}$. T_{ID} is an arbitrary but unique identifier used to identify messages. $Trigger$ defines when the aggregation will be conducted: periodically at a certain frequency, upon the connector's request, or at a particular time. $Data$ defines what information from the local smart grid will be collected in the aggregation, e.g. current power usage reading. $Collect$ tells a smart meter to wait for the input from a specific set of nodes (e.g. its children in the aggregation tree). $Operation$ tells a smart meter what operation to be performed, including pre-processing, encryption and operations for aggregation. $Destination$ is the parent node, i.e. to whom the output from $Operation$ will be submitted. And finally Key is a set of keys to be used for encryption. In Paillier cryptosystem, Key is a public key from the collector to be used to encrypt the local data.

Please note that not all the fields in the operation plan are mandatory. For instance, $Trigger$ could be omitted for an one-time aggregation that is conducted instantly –upon receipt of the operation plan. When the aggregation only covers a subset of the entire graph, the $Data$ field is blank for the meters that do not participate in the aggregation. Key could be omitted when the public key of the collector device is used for encryption. Please also note that $Trigger$ defines the time of local data reading, not the time of aggregation. Therefore, it guarantees, in time-sensitive tasks, no mis-synchronization will be caused due to the latency in computing or network communication.

As we have introduced, homomorphic encryption will be used at each participating smart meter. The collector translates operations on the plaintext to operations on the ciphertext. For instance, additions on the plaintext will be converted to multiplications on the ciphertext in the Paillier cryptosystem.

Example 3 *To calculate the total output power (in KW) at time t_0 in the entire neighborhood, the aggregation plan at node 9 is: $\{tid, t_0, \texttt{power}, \{N_5, N_8\}, Enc_K(power) \times I_5 \times I_8, N_{11}, K\}$.*

When a smart meter in the network receives the operation plan, it follows the following protocol

1) The smart meter determines if it should start the aggregation immediately, or wait for the trigger.
2) When an aggregation is to be performed, the smart meter retrieves local data as requested in $Data$ field of the plan, and encrypts it with Key as local input.
3) Then the smart meter waits for the inputs from the child nodes, as defined in $Collect$. Once receiving all the inputs, it follows $Operation$ to perform aggregation over all the input ciphertext.
4) Finally, the smart meter sends the output from Step 3 to the $Destination$ node, i.e. its parent node in the aggregation tree. The output message is constructed as $\{T_{ID}, TS, Data\}$, where TS is the timestamp of local data retrieval in Step 2. This timestamp is used for synchronizing different occurrences of repeating tasks.

We continue with Example 3 to further demonstrate the operations at node 9 and the collector device. In the following examples, C_{p_i} denotes the ciphertext of the local reading of node i, and C_{o_i} denotes the final output from node i.

Example 4 *When node 9 receives the aggregation plan, it first retrieves its own* `power` *reading at time t_0 and encrypts the reading with K to get local input $C_{p_9} = E_K(P_9)$. Node 9 then waits for the input from node 5 and 8. After receiving C_{o_5} and C_{o_8}, node 9 calculates $C_{o_9} = C_{p_9} \times C_{o_5} \times C_{o_8}$, and submits C_{o_9} to node 11.*

Example 5 *In this aggregation, the collector device receives inputs from nodes 11, 12, 15, 16, and 17. It computes* $C_{col} = C_{o11} \times C_{o12} \times C_{o15} \times C_{o16} \times C_{o17}$. *Further decomposing* C_{o11}, C_{o12}, *etc, we have:*

$$\begin{aligned} C_{col} &= C_{o11} \times C_{o12} \times C_{o15} \times C_{o16} \times C_{o17} \\ &= (C_{p11} \times C_{o9} \times C_{o10}) \times (C_{p12} \times C_{o13}) \times \\ &\quad (C_{p15}) \times (C_{p16} \times C_{o14} \times C_{o18}) \times \\ &\quad (C_{p17} \times C_{o19} \times C_{o20}) \\ &= C_{p11} \times C_{p9} \times C_{p5} \times C_{p1} \times C_{p2} \times ... \times C_{p20} \end{aligned}$$

Finally, the collector decrypts C_{col} *to obtain the aggregation result* $D(C_{col}) = P_{11}+P_9+P_5+P_1+P_2+...+P_{20} = \sum_{i=1}^{20} P_i$.

D. Analysis

Now we compare the complexity of the in-network aggregation approach (with homomorphic encryption) presented in this paper to the traditional aggregation approach, which collects the input from every smart meter and performs the aggregation at the collector device. We will compare from several dimensions including network traffic, system scalability, system robustness, security and privacy, and the overall computation.

Network: In the traditional approach, messages from all smart meters are routed to the collector device simultaneously. The average number of hops for each message to be transmitted to the collector device, $\overline{h}$, is determined by the size of the neighborhood (the residential area covered by a particular collector), the wireless communication range of each smart meter, and the routing scheme. Assume the number of nodes in the graph is N. To transmit data from all the smart meters participating in the aggregation, the total load on the network will be $\overline{h} * N$ hops. However, in the proposed in-network aggregation approach, the total load will be N hops.

Example 6 *In the example neighborhood, if we use the traditional aggregation approach to collect data from all the smart meters, the total load on the network will be 50 hops. On the other hand, the in-network aggregation approach only needs 20 hops in total. By choosing in-network aggregation, we saved 60% of network load. In real world cases, a collector device often covers a large neighborhood, which indicates a large* $\overline{h}$, *and therefore more savings on network load.*

Scalability, bottleneck and robustness: As we have shown, the overall system scalability highly depends on the smart meter network topology. In a well-designed network, the aggregation tree is usually wide and shallow, which makes our approach very scalable. The longest path in an aggregation process is the graph diameter, which usually grows at a speed of $\sqrt{N}$. Also, since most of computation are distributed to smart meters, with re-balance scheme, there is almost no unavoidable bottleneck in the in-network aggregation approach. On the contrary, most of the computation in the traditional approach are centralized at the collector device. Considering decrypting messages from all the smart meters is highly computation-intensive, the collector becomes the major bottleneck, especially when the number of smart meters in the neighborhood (N) gets large.

In in-network aggregation, when one smart meter fails, the failure will be detected immediately by its parent in the aggregation tree and reported to the collector. Then, the collector will update the aggregation tree and re-issue the query. The recover process will fail only when the aggregation graph becomes unconnected (e.g. split into two isolated subgraphs), which is often caused by the failure of a large number of nodes. Obviously, in such cases, most approach will also fail.

Security and privacy analysis: The Paillier cryptosystem adopted in in-network aggregation approach is semantically secure (IND-CPA): polynomial time adversary who intercepts the communication cannot derive significant information about the plaintext from the ciphertext and the public key. Meanwhile, with the existence of the random blinding factor r, the same data will be encrypted to different cipher with different r, which makes the approach resilient to the dictionary attack.

All homomorphic encryption systems are malleable – given the cipher and public key, an adversary could generate another cipher which decrypts to another meaningful plaintext in the same domain as the original plaintext. As a result, a dishonest or fake smart meter could falsify the data, which causes inaccurate aggregation result. However, this problem is not introduced by in-network aggregation, considering a dishonest smart meter could falsify its data in any aggregation approach. The problem could be solved by increasing the physical and software security of smart meters and improving authentication. Although we do not consider false data injection attack in this paper, detecting manipulation of the aggregate by the adversary is part of our future work.

Computation: The choice of encryption/decryption scheme has a strong impact on the computation at both smart meters and the collector. In particular, asymmetric encryption is more computationally expensive than symmetric encryption (e.g. AES and triple-DES). Here, we compare the computation load at both smart meters and the collect in two approaches. In the traditional approach, with no in-network aggregation, each smart meter will encrypt its message once with the public key, while the collector needs to decrypt N messages. In the proposed approach, every smart meter needs to encrypt the message once with homomorphic encryption (still asymmetric encryption), but the collector device only needs to apply one asymmetric decryption (to the final aggregation result). Moreover, the in-network aggregation approach distribute the computation of aggregation at the collector (e.g. the addition on the plaintext) to intermediate smart meters, and introduces extra overhead (e.g. the multiplication on the ciphertext). However, such overhead is small and acceptable per smart meter. For instance, a smart meter with k children in the aggregation tree only needs to perform $k + 1$ multiplications for each aggregation, where k is usually small (controlled by the re-balance process).

V. Conclusion and future works

In this paper, we present in-network data aggregation for smart grids. In this approach, a spanning tree rooting at the collector device is constructed to cover all of the smart meters. Aggregation is performed in a distributed manner in accordance to the aggregation tree – each node collects data from its children, aggregates them with its own data, and sends the intermediate result to the parent node. Homomorphic encryption is employed to protect the privacy of the electricity usage information, so that inputs and intermediate results are not revealed to smart meters on the aggregation path, while the aggregation is still correctly performed.

In this paper, we have assumed honest but curious model for the smart meters. However, there could be adversaries that maliciously forge their own data to manipulate the aggregation results. Such adversaries and false data reports need to be detected through advanced auditing approaches, which is one of our ongoing research. Meanwhile, we also plan to further refine the algorithm and deploy it in a real world smart grid system.

VI. Acknowledgement

This work was supported by AFOSR FA9550-07-1-0527 (MURI), ARO W911NF-09-1-0525 (MURI), NSF CNS-0905131, and NSF CNS-0916469.

References

[1] S. Massoud Amin and B. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *Power and Energy Magazine, IEEE*, vol. 3, no. 5, pp. 34 – 41, 2005.

[2] J. Lu, D. Xie, and Q. Ai, "Research on smart grid in China," in *Transmission Distribution Conference Exposition: Asia and Pacific, 2009*, Oct. 2009, pp. 1 – 4.

[3] A. Johnson, "The history of the smart grid evolution at southern california edison," in *Innovative Smart Grid Technologies*, Jan. 2010.

[4] P. Wolfs and S. Isalm, "Potential barriers to smart grid technology in Australia," in *Australasian Universities Power Engineering Conference*, Sept. 2009, pp. 1 – 6.

[5] S.-Y. Son and B.-J. Chung, "A Korean smart grid architecture design for a field test based on power IT," in *Transmission Distribution Conference Exposition: Asia and Pacific 2009*, Oct. 2009, pp. 1 – 4.

[6] Y. Serizawa, E. Ohba, and M. Kurono, "Present and future ICT infrastructures for a smarter grid in Japan," in *Innovative Smart Grid Technologies*, Jan. 2010, pp. 1 – 5.

[7] A. Sensing, A. Bose, and W. Wittig, "Power system design: basis for efficient smart grid initiatives," *IET Seminar Digests*, vol. 2008, no. 12380, pp. 58–58, 2008.

[8] H. van Bruchem, "Think smart! The introduction of smart gas meters," in *23rd World Gas Conference*, 2006.

[9] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security Privacy, IEEE*, vol. 7, no. 3, pp. 75 –77, 2009.

[10] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *Security Privacy, IEEE*, vol. 8, no. 1, pp. 81 –85, 2010.

[11] W. H. Sanders, "Progress towards a resilient power grid infrastructure," in *Proceedings of the IEEE Power & Energy Society General Meeting*, July 2010.

[12] K. Moslehi and R. Kumar, "Smart grid - a reliability perspective," in *Innovative Smart Grid Technologies*, 2010, pp. 1–8.

[13] A. G. van Engelen and J. S. Collins, "Choices for smart grid implementation," *HICSS'10*, pp. 1–8, 2010.

[14] A. Bose, "Smart transmission grid applications and their supporting infrastructure," *IEEE Transactions on Smart Grid*, 2010.

[15] R. D. Tabors, G. Parker, and M. C. Caramanis, "Development of the smart grid: Missing elements in the policy process," in *43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–7.

[16] R. Schuler, "Electricity markets, reliability and the environment: Smartening-up the grid," in *43rd Hawaii International Conference on System Sciences*, 2010, pp. 1 –7.

[17] X. Wei, Z. Yu-hui, and Z. Jie-lin, "Energy-efficient distribution in smart grid," in *Sustainable Power Generation and Supply, 2009. SUPERGEN '09. International Conference on*, 6-7 2009, pp. 1 –6.

[18] B. Saint, "Rural distribution system planning using smart grid technologies," in *IEEE Rural Electric Power Conference*, 2009.

[19] M. Masoum, P. Moses, and S. Deilami, "Load management in smart grids considering harmonic distortion and transformer derating," in *Innovative Smart Grid Technologies*, 19-21 2010.

[20] A. Pasdar and S. Mirzakuchaki, "Three phase power line balancing based on smart energy meters," in *EUROCON 2009*, 2009, pp. 1876 –1878.

[21] B. D. Russell and C. L. Benner, "Intelligent systems for improved reliability and failure diagnosis in distribution systems," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 48 –56, june 2010.

[22] S.-W. Luan, J.-H. Teng, S.-Y. Chan, and L.-C. Hwang, "Development of a smart power meter for AMI based on ZigBee communication," in *PEDS 2009*, 2009, pp. 661 –665.

[23] V. Sood, D. Fischer, J. Eklund, and T. Brown, "Developing a communication infrastructure for the smart grid," in *Electrical Power Energy Conference (EPEC), 2009 IEEE*, oct. 2009, pp. 1 –7.

[24] G. Srinivasa Prasanna, A. Lakshmi, S. Sumanth, V. Simha, J. Bapat, and G. Koomullil, "Data communication over the smart grid," in *IEEE International Symposium on Power Line Communications and Its Applications*, 2009, pp. 273–279.

[25] A. Aggarwal, S. Kunta, and P. Verma, "A proposed communications infrastructure for the smart grid," in *Innovative Smart Grid Technologies*, Jan. 2010, pp. 1–5.

[26] A. Metke and R. Ekl, "Smart grid security technology," in *Innovative Smart Grid Technologies*, Jan. 2010, pp. 1–7.

[27] 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, June 2010.

[28] B. Krishnamachari, D. Estrin, and S. B. Wicker, "The impact of data aggregation in wireless sensor networks," in *Proceedings of the 22nd International Conference on Distributed Computing Systems*, 2002, pp. 575–578.

[29] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "Tag: a tiny aggregation service for ad-hoc sensor networks," *SIGOPS Oper. Syst. Rev.*, vol. 36, no. SI, pp. 131–146, 2002.

[30] C. Castelluccia, "Efficient aggregation of encrypted data in wireless sensor networks," in *In MobiQuitous*. IEEE Computer Society, 2005, pp. 109–117.

[31] J. Girao and D. Westhoff, "Cda: Concealed data aggregation for reverse multicast traffic in wireless sensor networks," in *In IEEE International Conference on Communications (ICC05), Seoul, Korea*, 2005.

[32] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 278–287.

[33] K. B. Frikken and J. A. Dougherty, IV, "An efficient integrity-preserving scheme for hierarchical sensor aggregation," in *Proceedings of the first ACM conference on Wireless network security*, 2008, pp. 68–76.

[34] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in cryptology*. Springer-Verlag New York, Inc., 1985, pp. 10–18.

[35] P. Paillier, "Public-key cryptosystem based on composite degree residuosity classes," in *Proceedings of Eurocrypt '99*, 1999.

[36] D. Naccache and J. Stern, "A new public key cryptosystem based on higher residues," in *CCS '98: Proceedings of the 5th ACM conference on Computer and communications security*, 1998, pp. 59–66.

[37] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in *Proceedings of Theory of Cryptography (TCC)*, 2005, pp. 325–341.

[38] P. Paillier and D. Pointcheval, "Efficient public-key cryptosystems provably secure against active adversaries," in *Advances in Cryptology – Proceedings of Asiacrypt '99*. Springer-Verlag, 1999, pp. 165–179.

[39] O. Goldreich, *Foundations of Cryptography: Volume II (Basic Applications)*. Cambridge University Press, 2004.

[40] R. Brown, "Impact of smart grid on distribution system design," in *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, july 2008, pp. 1 –4.