AgSec: Secure and Efficient CDMA-based Aggregation for Smart Metering Systems

Navid Alamatsaz, Arash Boustani, Murtuza Jadliwala, and Vinod Namboodiri
Wichita State University, Wichita, Kansas 67260, USA
Email: {nxalamatsaz,axboustani,murtuza.jadliwala,vinod.namboodiri}@wichita.edu

***Abstract*— Security and privacy concerns in the future power grid have recently received tremendous focus from security advocates. Most existing security mechanisms utilize cryptographic techniques that are computationally expensive and bandwidth intensive. However, aggregating the large outputs of these cryptographic algorithms has not been considered thoroughly. Smart Grid Networks (SGN) generally have limitations on bandwidth, network capacity and energy. Hence, utilizing data aggregation algorithms, the limited bandwidth can be efficiently utilized. Most of the aggregation algorithms use statistical functions such as minimum, maximum, and average. before transmitting data over the network. Existing aggregation algorithms, in SGNs, are generally expensive in terms of communication overhead, processing load and delay. However, our proposed CDMA-based data aggregation method provides access to all the data of all the smart meters in the root node, which in this case is the Utility Center, while keeping the smart metering data secure. The efficiency of the proposed method is confirmed by mathematical analysis.**

I. INTRODUCTION

Millions of people suffered from the biggest blackout in North American history in 2003. Investigations showed that the outage was because of lack of real-time monitoring and diagnosis and failure in proper load balancing [1]. Recently *Smart Grid* has been proposed as the next generation power grid. A Smart Grid is an electrical grid that utilizes communication technologies and information processing to collect, process and act on gathered information in order to improve reliability, efficiency, economics and sustainability of the power grid [2]. This will help the utility companies to act on consumer information gathered from smart meters (SM) at the user's premises. The two-way communication capability will enable functions such as demand-response, demand-dispatch, self-monitoring, and self-diagnosis for the existing power grid [3]. It also promises reduced prices through dynamic pricing schemes, wide penetration of renewable resources such as wind and solar, and fewer power outages [4].

Smart Grid researchers have been studying miscellaneous problems such as communication technologies and infrastructure [5]-[9], legal and policy concerns [10], [11], reliability, failure diagnosis and recovery [12]-[14], demand-response, load-shaping and peak-shaving [15]-[17], data aggregation [5], [18]-[20] and, last but not the least, security and privacy [3]-[5], [21]-[23]. Having access to fine-grained usage data reveals serious potential security and privacy threats to the users. For instance, it can be easily determined if a residential house is vacant or not by observing the fine-grained energy consumption patterns [24]. It is also possible to track the location of the residents of a house based on the appliance they are using [25]. Insurance companies can monitor and track eating, sleeping and possibly exercise habits of a household [26], [27]. In 2009, the Dutch Parliament prohibited the utilization of smart meters because of privacy issues. There are also many cyber security related challenges for the deployment of the Smart Grid [5]. The concept of Smart Grid is about "moving from a relatively small number of carefully controlled devices to an Internet-like distributed environment". This "Internet-like distributed environment" is vulnerable to many known and unknown cyber security attacks [28]. The security threats to the Smart Grid can target the confidentiality and the integrity of the gathered fine-grained user data. They can also threaten the availability of the power grid. Computerworld [29] reports more than 170 outages caused by cyber-security attacks. It goes without saying that without proper security and privacy-preserving mechanisms, large scale deployment and proliferation of the Smart Grid is difficult. Earlier security approaches have primarily used cryptographic techniques such as homomorphic encryption and secure multiparty computation in order to preserve user privacy while aggregating usage data [30]. These approaches, although providing strong guarantees of confidentiality, are very heavy from a computational and communicational stand-point and may not be feasible on low-end smart meters with limited computation capabilities. Homomorphic cryptosystems usually generate an output of a huge fixed-length compared with the data generated by smart meters. This ciphertext can be up to one hundred times larger than the actual smart metering data [5]. Given the frequency of the data being sent and possible bandwidth limitations, this can lead to unacceptable delay and network overhead.

In this paper, we investigate the feasibility of existing privacy-preserving data aggregation approaches. We devise a new efficient and computationally feasible secure data aggregation technique for smart meters using coding theory and spread spectrum technologies.

The rest of the paper is organized as follows. Related work in the literature and background on existing secure aggregation schemes is outlined in Section II. The network and adversary model assumed in this work along with basics of coding theory are presented in Section III. Our proposed CDMA-based secure aggregation protocol is outlined in Section IV, and mathematical evaluation and results are discussed in Section V. We conclude the paper with a summary of contributions and results in Section VI.

This work was supported in part by the Power Systems Engineering Research Center (PSERC) Project S-54.

978-1-4799-2355-7/14/$31.00 ©2014IEEE

II. BACKGROUND AND RELATED WORK

Below we outline existing cryptographic approaches to private data aggregation in Smart Grid Networks (SGN) and also study some data aggregation methods in other networking infrastructures with similar constraints such as WSNs.

A. Homomorphic Encryption for Secure Communication

A public-key cryptosystem is known to have homomorphic properties if $E(m_1 \lozenge m_2) = E(m_1) \vartriangle E(m_2)$, where E is the encryption function, and $\lozenge$ and $\vartriangle$ are two different mathematical operations. Based on the supported operations, homomorphic cryptosystems fall into two broad categories: partially homomorphic and fully homomorphic. Partially homomorphic cryptosystems only support either addition or multiplication or in some cases polynomials up to certain degrees, whereas fully homomorphic cryptosystems support both addition and multiplication [5], [23]. We refer the readers to [31]-[34] for more details on homomorphic cryptosystems.

In SGNs, the utility companies are interested in statistics such as total consumption for billing in a specific time period [5]. Given that sum of consumed electricity of all smart meters in a residential neighborhood is of interest to the UC, homomorphic properties of the Paillier [34] encryption can be useful. Rather than adding the consumption data in plaintext, one can multiply the encrypted values and then decrypt the result to get the addition of plaintext data.

He et al. [23] present a secure data exchange scheme for the smart grid based on homomorphic properties of Goh cryptosystem [35]. Goh supports an arbitrary number of additions and a single multiplication on the ciphertext. It is worth noting that the aforementioned protocol is only a secure data communication scheme without any aggregation capabilities. Li et al. [18] utilize the homomorphic properties of Paillier to propose an incremental data aggregation scheme. In [18] every node passes its encrypted consumption data to its parent node on the aggregation tree. The parent node multiplies the received value into its own encrypted consumption data and passes the total result to the next parent node. Therefore, all the meters participate in the aggregation, without seeing any intermediate or final result. Garcia and Jacobs [36] present a privacy-preserving protocol using Paillier based on secret sharing. Their proposal hides consumption data from the Utility Center (UC) as it receives random shares of data which it cannot decrypt. The other nodes cannot retrieve meaningful information either since they only receive random shares. Kursawe et al. [37] propose two approaches to calculate total consumption in SGN. In their first approach, called *aggregation protocols*, smart metering data are masked in such a way that after summing the data from all smart meters masking values cancel each other out and the UC gets the total consumption information. In their second approach, named *comparison protocols*, they consider that the UC roughly knows the total consumption. Erkin and Tsudik [38] propose a cryptographic protocol based on a modified version of the Paillier cryptosystem to calculate the total consumption of all the SMs in a given neighborhood as well as a single SM in an Advanced Metering Infrastructure (AMI). Acs and Castelluccia [39] suggest a solution using masking and differential privacy and utilizing the homomorphic properties of a computationally-cheap cryptosystem for private data aggregation. Lu et al. [40] propose an *Efficient and Privacy-Preserving Aggregation (EPPA)* for smart grid communications by structuring multidimensional data and encrypting them with the Paillier cryptosystem. Erkin et al. [5] study different existing secure signal processing mechanisms in SGNs and compare different existing cryptographic methods in terms of computational complexity, efficiency and imposed overhead.

B. Data Aggregation Methods

He et al. [41] and Li et al. [42] propose similar integrity preserving data aggregation schemes, *iPDA* and *EEHA* respectively, for wireless sensor networks using the concept of data slicing and assembling. The authors propose three steps: i) Constructing an aggregation tree using the well-known *LEACH* algorithm [43]. ii) Segmenting or slicing the data, and iii) merging the pieces of data at the aggregator and sending the merged data to the sink node. *iPDA* uses multiple aggregation trees, hence providing better integrity level, by sending more than one copy of the data to the destination. However, transmitting more than one copy of the same data can cause extra communication overhead. Zanjani et al. [44], [45] propose a new energy-efficient aggregation mechanism for WSNs using the concepts of coding theory. The sensor nodes are assigned unique Orthogonal Chip Sequences (OCS) that are used to code and send their data on the CDMA channel. The authors claim that, utilizing *ESTOC*, data integrity can be protected while aggregating. Also, *ESTOC* reduces Bit Error Rate (BER) and interference caused by simultaneous transmission of nodes. Yan et al. [19] propose a secure in-network data aggregation scheme to aggregate the data from smart appliances inside a Home Area Network (HAN). Similar to *ESTOC* [44], the authors in this scheme utilize the properties of spread spectrum communications for efficient aggregation.

C. Discussion

In the cryptographic approaches discussed in [5], [18], [23], [36]-[38], we observe that the power-usage information is generally of small size (e.g. 20 bits) [40], [3]. However, the plaintext input size of most existing homomorphic cryptosystems is huge [5], [40], for example 2048 bits for the widely-used Paillier cryptosystem [34], [36], [38], [40]. As a result, the input data has to be padded before encryption. Given the high frequency of data collection and the number of deployed smart meters, this will result in unacceptable communication overhead on the network, and also high processing burden on the smart meters with limited computational capabilities [40]. Aggregation schemes that construct and utilize the spanning-tree, for instance by Li et al. [18], also do not consider performance issues. The processing and communication overhead makes the protocol less suitable in practical implementations. Moreover, depending on the depth of the spanning tree of the network, there can be large delays between the time power consumption data is reported by the meters and the time the aggregated data is received at the UC.

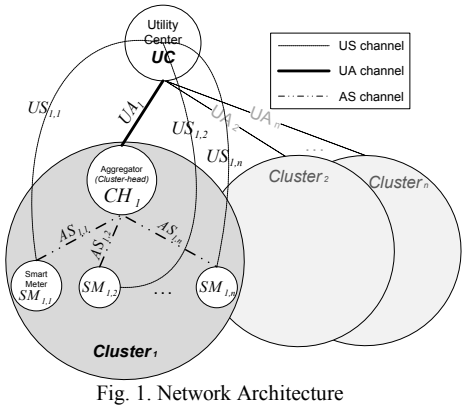

Fig. 1. Network Architecture

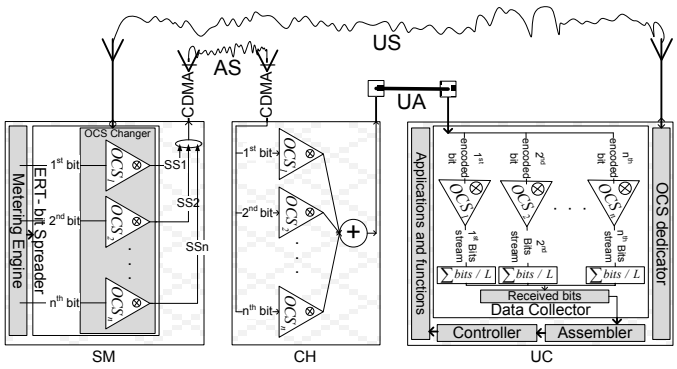

Fig. 2. Participating Entities in Secure Aggregation

The aggregation schemes proposed in [41]-[45] do not consider any security issues. The main focus of the authors is increasing data integrity and energy efficiency in WSNs. Phulpin et al. [47] study the efficiency and benefits of network coding in both PLC and wireless SGNs. The authors also show that using coding theory in SGN reduces the delay by decreasing the number of time slots and saves energy through reducing the number of transmission.

We are proposing a secure aggregation scheme using coding theory and spread spectrum utilizing slicing and assembling [41], [42] to efficiently aggregate energy usage while improving network performance and decreasing unnecessary loads on smart meters. Our contention-free scheme will also decrease the delay, BER, and interference.

III. NETWORK ARCHITECTURE

A. Network and Communication Model

We consider the widely-used wireless-wired architecture for the deployment of SGN. The wireless communication between smart meters, which are organized into clusters, and the aggregator or Cluster Head (CH) uses 802.15.4 or Zigbee due to characteristics such as low power, short delay, self-organization, scalability, and high security [8]. The aggregated data will be forwarded from the CH to the UC using a dedicated point-to-point wired link.

Figure 1 depicts a three-level hierarchical network architecture. The communication between the UC and the i^{th} aggregator is denoted as UA_i. Similarly $AS_{i,j}$ represents the communication between the i^{th} aggregator and the j^{th} smart meter in the i^{th} cluster. The control and signaling messages between the UC and the j^{th} smart meter in the i^{th} cluster are exchanged on a channel referred to as $US_{i,j}$. The signaling messages, which are used in the initialization phase, are discussed in details in section IV-A. The Zigbee medium access protocol on all *AS* channels is CDMA. Also all *UA* communications are on a dedicated wired channel. Finally, our signaling channel is a high-range wireless WAN technology, such as GPRS, UMTS or LTE. Figure 2 illustrates the components implemented in different network entities.

B. Communications on the CDMA Channel

All communication takes place over three separate channels as discussed in section III-A. All smart meter data from the smart meter to the aggregator are sent over the CDMA-based data channel, represented as the AS channel (in Fig. 1). The OCSs for encoding data transmission on the *AS* channel are generated using the Golay code generation algorithm [46]. The most important characteristics of OCSs that should be considered before choosing an algorithm are auto/cross correlation, length of the generated OCSs versus the number of possible OCSs, and fault tolerance capabilities. Golay OCSs can be generated recursively, as shown in Eqn. 1.

$$C_L = \begin{bmatrix} C_{\frac{L}{2}} & C_{\frac{L}{2}} \\ C_{\frac{L}{2}} & -\bar{C}_{\frac{L}{2}} \end{bmatrix} \qquad \forall L = 2^M, \quad M \geq 1, \; C_1 = \bar{C}_1 \tag{1}$$

$$when \quad C_L = [A_L \quad B_L] \qquad and \qquad \bar{C}_L = [A_L \quad -B_L]$$

In Eqn. 1, $L = 2^M$ is the total number of available OCSs, where $M \geq 1$ is the number of bits in each OCS. A_L and B_L are $L \times L/2$ sub-matrices.

Let us assume that time is divided into periods of random length denoted by a random variable ψ . During each period, each smart meter is assigned a subset of OCSs for use in that period by the UC. The assignment happens over the *US* signaling channel. The communications over the *US* channels are secured using symmetric key cryptography and shared keys between the smart meter and UC based on what has been proposed in [18], [31], [36]. The OCSs for each smart meter are randomly selected by the UC from a large pool of available OCSs. Each smart meter will use the OCSs uniquely assigned to it in the time frame ψ. In order to spread data bits on the *AS* data channel, the smart meter calculates the inner-product of every data-bit in appropriate OCS. Every single bit of data is coded independently with an OCS different from the previous and next data bit. This will build the foundation of our secure scheme as described in section IV-B. It should be noted that it is possible for multiple smart meters to use the same OCS for data transmission in different parts of the network as long as they are not in the same cluster.

C. Adversary Model

In any networking scenario, all individuals in the network can fall into three broad categories based on their behavior. (i) honest entities that fully follow the rules of the established protocol. (ii) malicious or cheating nodes that not only do not follow the protocol but also try to manipulate, forge or deny access to possible resources. (iii) semi-honest or honest-but-

curious nodes follow the defined protocols but they will, or they can, infer privacy-sensitive data. In our proposed scheme we consider the UC as the only honest party. The aggregators are assumed to follow the semi-honest model. The neighboring SMs are, generally, semi-honest; however there can be some malicious nodes in the vicinity. Our objective is to completely secure all the communications from malicious and semi-honest nodes against possible sniffing, spoofing, and inference attacks.

IV. Secure Aggregation using Coding Theory

A. Initialization Phase

Upon initial deployment, the UC communicates control information to each smart meter through the WAN interface on the *US* channel. For each time duration ψ_i, the UC assigns each smart meter, SM_j, a set of attributes including, a temporary eight-bit identifier ($ID_{i,j}$) and a group of valid OCSs, denoted by $G_{O,i}^{j} = \{OCS_1^j, OCS_2^j, ..., OCS_g^j\}$. The integrity, authenticity and confidentiality of the communication between the UC and the SMs are ensured using appropriate cryptographic techniques. In this phase every smart meter gets the information required for data transmission on the CDMA channel in the next *t* time-slots, as illustrated in Fig. 3. It should be noted that, as this is a one-time process in every *t* time slots and $\psi_t \gg \psi_i$, the imposed overhead is negligible. Also we are not including any frame-level error checking mechanisms such as CRC because spread spectrum, by nature, can tolerate fault up to a certain level.

B. Proposed Secure Aggregation Protocol(AgSec)

After all smart meters are configured with appropriate OCS and ID information; they start to transmit their readings every τ seconds [3]. Different time intervals, ranging from 30 seconds to a few hours, could be found in the literature [3]. Each node *j* is assigned a group of OCSs ($G_{O,i}^{j}$) for each time interval ψ_i. The k^{th} bit of the data stream generated by *SMj* will be coded with $O^{j}_{(k \bmod g)}$, where *g* is the total number of OCSs assigned to SM_j in a given timeslot ψ_i. The OCS $O_i(t)$ assigned to any SM_i at any instant in time *t* can be represented as shown in Eqn. 2.

$$O_i(t) = \sum_{j=0}^{L-1} O_{(j,i)} . p(t - jT_c) \tag{2}$$

In Eqn. 2, *p(t)* is a rectangular pulse which is equal to 1 for $0 \le t < T_c$ and zero otherwise. T_c is the chip duration of the OCS and $O_{(j,i)}$ is the j^{th} bit of the OCS assigned to SM_i (from the set of all OCSs C_L). The signal generated after encoding a data symbol of SM_i with the corresponding OCS is given by

$$x_i(t) = f_i \sum_{j=0}^{L-1} O_{(j,i)} p(t - jT_c), 0 \le t < T_f \tag{3}$$

where, f_i is the data symbol of SM_i that needs to be encoded and $T_f = L.T_c$ is the duration of the encoded data symbol or data bit. The inner product of the sent bit with the OCS is done bit-synchronously. Then, the overall transmitted signal *x(t)* of all *n* smart meters in a cluster can be given by Eqn. 4 [46].

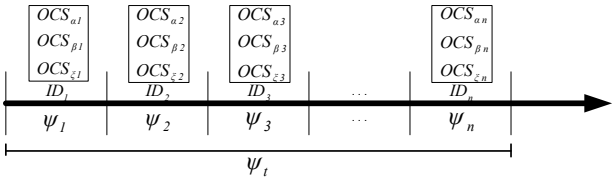

Fig. 3. Initialization Parameters

$$x(t) = \sum_{i=1}^{n} x_i(t) \tag{4}$$

CH will receive a signal including all the bits transmitted by all the smart meters. The received signal will be decoded by CH using all valid OCSs generated by the same algorithm with which they were initially produced by the UC. Given that SMs code their bits with different OCSs at every transmission it is impossible for the CH to decode and extract the actual data from the incoming signal. It should be noted that CH does not know the OCSs assigned to every single SM in the time period ψ_i, all it knows is a list of all possible OCSs in the network. Hence, after decoding the received signal it only has a bit-stream in which neither the IDs, nor the actual data, can be interpreted. After the decoding phase, CH has an *L* bit data stream for every available OCS. All corresponding bits of the decoded data with all possible OCSs will be added and placed in an *L*-element array. Each element of the array is between *–L* and *+L*. The produced array will be sent to the UC as a whole piece of data on the dedicated point-to-point *UA* link.

After the array is received at the UC it is easily decoded and interpreted into actual data transmitted by smart meters. Since UC maintains a table of assigned OCSs (in the same order that was agreed in the initialization phase) and IDs to every single SM in the network, it is able to retrieve the actual data by using appropriate OCS for every bit. We would like to note that the mentioned process is performed on the actual received data in upper layers rather than the physical layer.

Also, we would like to argue that the possible malicious nodes in the network are not able to sniff or spoof any information. Given that every single bit of the data is coded with a different OCS, even if packets are captured, they cannot be decoded. The only entity in the network that knows about the set of assigned OCSs to the smart meters is the UC. Hence, all communications will be secured; and privacy–sensitive information cannot be inferred. Our proposed secure aggregation technique is outlined in protocols 1, 2 and 3.

```
1: Function (US operation)
2:   For each period ψk do
3:       Generate OCS table with Golay algorithm;
4:       Function (Initialization);
5:       Function (UA data channel);
6:   End For
7: End Function
8: Function (initialization)
9:     Establish a safe communication with each SM;
10:    Generate random SM ID;
11:    OCS dedicator unit grant some OCSs to each SM;
12:End function;
13:Function (UA data transmission)
```

```
14:    While data on UA channel do
15:        For (all valid OCS)
16:            Decode each received bit stream on a
               particular OCS by inverse inner product;
17:        End for
18:        Collect all data bits;
19:        Assemble bits based on ID & OCS;
20:    End while;
21:    Controller check decrypted data for being in
       thresholds;
22:    Utilize the aggregated data;
23:End function;
```

Protocol 1: UC functions

```
1: While data on CDMA data channel do
2:        Receive all signals from different carriers;
3:        Calculate the SUM of each corresponding bits'
          column of OCSs;
4:        Send calculated SUM values to UC on
          point-to-point channel;
5: End while
```

Protocol 2: CH functions

```
1: Function (SM operation)
2:   While network is ON do
3:      Function(US data)
4:      Function (Metering Engine);
5:   End While
6: End Function
7: Function (US data)
8:    While data on US control channel do
9:       If (receive signal come from UC) then
10:           Update OCSs' table and their orders;
11:      End if
12:   End while
13:End Function
14:Function (Metering Engine)
15:   While (Metering Engine produce value) do
16:      Get a OCS from OCS changer ;
17:      ADD, D random value to data frame;
18:      Encode k^th bit of data frame by (k mod g)^th OCS;
19:      Spread encoded bit stream on AS CDMA carrier;
20:   End while
21: End Function
```

Protocol 3: SM functions

V. EVALUATION AND RESULTS

As discussed in section II-A, existing secure aggregation schemes impose a significant communication and computation overhead on SGNs with limited capabilities. Aggregation schemes that take advantage of the homomorphic properties of cryptosystems require fixed large size input blocks which is not ideal for small-sized data generated by SMs. The 20 to 30 bit [5] output data generated by SMs has to be padded, e.g., to 2048 bits for Paillier [34], before encryption. In our approach, by choosing OCSs with appropriate length, this overhead can be significantly reduced. Readers should note that in our scheme each bit will be spread to L bits after encoding.

We are evaluating our results with clusters of ten and also twenty smart meters and assuming that each smart meter is assigned three OCSs to use in every given time slot. Hence, using an OCS with L=32 and L=64 will be ideal for each scenario, respectively. The OCS length L limits the maximum number of users per cluster to $\frac{L}{|G_{O,i}^{j}|}$. The number of total users in the network is independent from the OCS structure used.

$$D_T = \frac{(F+H_{ID}) \times L}{R} \quad (5)$$

where F is the frame length, H_{ID} is the ID header, L is the OCS length and R is the link bit-rate. Given Eqn. 5, the transmission delay using L=32 and L=64, assuming a 200 kbps ZigBee link, is 4.8 *ms* and 9.6 *ms*, respectively. However, using traditional homorphic cryptosystems as proposed by [18], we have:

$$D_T = \frac{(H_{ID}+D_C+T_{CRC})}{R} \quad (6)$$

where H_{ID} is the identifier header, D_C is the encrypted data (payload) and T_{CRC} is the error-checking trailer. Given the values used in [3], the transmission delay will be 10.44 *ms*. Hence, using an OCS with appropriate length we were able to decrease the overhead significantly, as seen in Table I. It should be noted that we are only considering the transmission delay. Moreover, given the high processing load and queuing delays due to the non-simultaneous transmission and high BER and retransmissions, the overall delay of the homomorphic approaches are too high compared with *AgSec*. Table I summarizes the transmission delay and total *communication overhead* $= \frac{Transmitted\ Data}{Actual\ Data}$ for one smart meter.

Another shortcoming of the secure homomorphic aggregation schemes, such as [18], is that every node's data should be passed hierarchically to the upper level node in the aggregation tree. This process continues until all the data is aggregated at the UC. However, this can increase the total delay which depends on the height of the aggregation tree. Our approach overcomes this issue as all nodes are able to transmit their data simultaneously and independently.

TABLE I. TRANSMISSION DELAY AND COMMUNICATION OVERHEAD

	AgSec L=32 bits	**AgSec L=64 bits**	**Homomorphic (Paillier)**
Transmission Delay (ms)	4.8	9.6	10.44
Communication Overhead	43.63	87.26	94.91

Moreover cryptographic solutions usually have high processing which is not suitable for smart meters with resource constrained processors. However, our secure aggregation protocol does not put extra processing burden on the smart meters as it only requires basic addition and multiplication which can be done efficiently at the circuit level.

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented a new approach for securing data aggregation in smart metering systems. Our proposed approach uses a coding theory based strategy which uses spread spectrum communications on a CDMA channel to securely aggregate sensitive power consumption data from smart meters. Our analysis showed that, provided appropriate parameters are chosen, our proposed technique imposes lesser delay and overhead on SGNs as compared to cryptographic approaches. The proposed method uses code division multiplexing to enable simultaneous transmissions, reduce bit

error rate and interference. As part of future work, we are planning to implement the proposed scheme in a real test-bed of SMs to analyze its security and efficiency in practice.

REFERENCES

[1] Blackout 2003, Independent Electricity System Operator, 2012.

[2] U.S. Department of Energy. "Smart Grid, Department of Energy", 2012.

[3] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser, "Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems," *CCS '12*, USA, Oct 2012.

[4] A. Barenghi, and G. Pelosi, "Security and Privacy in Smart Grid Infrastructures," *DEXA'11*, France, Aug 2011.

[5] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-Preserving Data Aggregation in Smart Metering Systems: An overview," *IEEE Signal Processing Magazine'13*, Mar 2013.

[6] A. G. van Engelen and J. S. Collins, "Choices for smart grid implementation," *HICSS'10*, 2010.

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

[8] F. R. Yu, P. Zhang, X. Weidong, and P. Choudhury, "Communication systems for grid integration of renewable energy resources," *IEEE Network Magazines'11*, 2011.

[9] R. Amin, J. Martin, and X. Zhou, "Smart Grid Communication using Next Generation Heterogeneous Wireless Networks," *SmartGridComm'12*, Taiwan, Nov 2012.

[10] R. D. Tabors, G. Parker, and M. C. Caramanis, "Development of the smart grid: Missing elements in the policy process," *HICSS'10*, 2010.

[11] R. Schuler, "Electricity markets, reliability and the environment: Smartening-up the grid," *HICSS'10*, 2010.

[12] D. Niyato, P. Wang, and E. Hossain, "Reliability Analysis and Redundancy Design of Smart Grid Wireless Communications System for Demand Side Management," *IEEE Wireless Communications Magazine*, 2012.

[13] B. Falahati, Y. Fu, and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," *IEEE Transaction on Smart Grid*, 2012.

[14] K. Moslehi, and R. Kumar, "A Reliability Perspective of the Smart Grid," *IEEE Transaction on Smart Grid*, Jun 2010.

[15] S. Shao, M. Pipattanasomporn, and S. Rahman, "Demand Response as a Load Shaping Tool in an Intelligent Grid With Electric Vehicles," *IEEE Transaction on Smart Grid*, Dec 2011.

[16] S. Shao, M. Pipattanasomporn, and S. Rahman, "Grid Integration of Electric Vehicles and Demand Response with Customer Choice," *IEEE Transaction on Smart Grid*, Mar 2012.

[17] I. C. Paschalidis, B. Li, and M. C. Caramanis, "Demand-Side Management for Regulation Service Provisioning Through Internal Pricing," *IEEE Trans. on Power Systems*, Aug 2012.

[18] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," *IEEE SmartGridComm'10*, USA, Oct 2010.

[19] Y. Yan, Y. Qian and H. Sharif, "A Secure Data Aggregation and Dispatch Scheme for Home Area Networks in Smart Grid", *IEEE Globecom'11*, USA 2011.

[20] A. Bartoli, J. Hernández-Serrano; M. Soriano; M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," *SmartGridComm'10*, USA, 2010.

[21] H. S. Fhom, and K. M. Bayarou, "Towards a Holistic Privacy Engineering Approach for Smart Grid Systems," *IEEE TrustCom'11*, China, Nov 2011.

[22] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber Security Challenges in Smart Grids," *ISGT'11*, UK, Dec2011.

[23] X. He, M. Pun, and C. -C. J. Kuo, "Secure and Efficient Cryptosystem for Smart Grid Using Homomorphic Encryption," *IEEE ISGT'12*, USA, Feb 2012.

[24] M. Lisovich and S. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems," *Clemson University Power Systems Conference*, 2008.

[25] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security and Privacy*, 2010.

[26] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, & D. Irwin, "Private memoirs of a smart meter," *ACM BuildSys*, 2010.

[27] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, 2009.

[28] F. Cohen, "The Smarter Grid," *IEEE Security & Privacy*, 2010.

[29] Computerworld magazine, "Stuxnet renews power grid security concerns", Jul 2010.

[30] R. Lagendijk, Z. Erkin, M. Barni, "Encrypted signal processing for privacy protection," *IEEE Signal Process. Mag.*, 2013.

[31] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, Feb 1978.

[32] C. Gentry, "Fully homomorphic encryption using ideal lattices," *STOC'09*, USA, 2009.

[33] M. V. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," *ACM EUROCRYPT*, 2010

[34] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *ACM EUROCRYPT*, 1999.

[35] E.-J. Goh, "Encryption Schemes from Bilinear Maps," *Department of Computer Science, Stanford University*, 2007.

[36] F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," *STM*, 2010.

[37] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," *HotPETs'11,* Canada, 2011.

[38] Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," *ACNS*, 2012.

[39] G. Ács and C. Castelluccia, "I have a DREAM! (Differentially PrivatE smart Metering)," *ACM IH'11*, May 2011.

[40] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Transactions on Parallel and Distributed Systems*, 2012.

[41] W. He, H. Nguyen, X. Liu, K. Nahrstedt and T. Abdelzaher, "iPDA: An Integrity-Protecting Private Data Aggregation Scheme for Wireless Sensor Networks", *IEEE WCPS*, 2009.

[42] H. Li, K. Lin and K. Li, "Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks," *ACM Journal Computer Communications*, 2011.

[43] C. Weng, M. Li and X. Lu, "Data Aggregation with Multiple Spanning Trees in Wireless Sensor Networks", *ICESS*, 2008.

[44] M.B. Zanjani, R. Monsefi and A. Boustani, "Energy Efficient/highly Secure Data Aggregation Method using Tree structured Orthogonal Codes for Wireless Sensor Network," *IEEE ICSTE'10*, USA, 2010

[45] M. B. Zanjani, A. Boustani, "Energy aware and highly secured data aggregation for grid-base Asynchronous wireless sensor network," *IEEE Pacrim*, Canada, 2011.

[46] H. H. Chen, "The Next Generation CDMA Technologies". John Wiley and Sons, 2007.

[47] Y. Phulpin, J. Barros, and D. Lucani, "Network Coding in Smart Grids," *IEEE SmartGridComm*, 2011.