International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Secure Data Aggregation Techniques in Smart Grid

Shital G Bhosle[1], Aarti A Agarkar[2]

[1, 2]Department of Information Technology, Sinhgad College Of Engineering,, Pune -411041, India

Abstract: ***Security is very important issues in data aggregation technique in smart grid systems. For efficient communication in smart grid systems network topology is also important factor. A home area network is basic data reading unit in smart grid. To achieve efficient communication in smart grid systems, appropriate network topology need to be selected. There is challenge in data aggregation because we have to make data aggregation secure without disclosing information during aggregation process and also obtain secure aggregated results. We described various protocols for data aggregation to be performed secured and network topologies in smart grid systems.***

Keywords: Smart Grid, Secure Data Aggregation, Wireless Sensor Network

1. Introduction

Smart grid can deal with two-way flow of both electricity and control messages for creating widely distributed power network which is automated in nature. Smart grid provides advantages in the area of communication networks by real-time monitoring and controlling the data. Smart grid system includes variety of nodes which can perform operations and measures on data that includes smart devices, smart meters, smart appliances, renewable energy and energy efficient resources. In electronic power systems control of consumption and production of electricity are important functions of smart grid. Two points that describes why smart grid is important:

1) Current electricity grids which are inadequate, outdated and aging needs to be improved so as to meet future electricity demand challenges.
2) The smart grid provides benefits in six key value area reliability, economy, security, efficiency, environmental and safety.

Following benefits are expected in smart grid system:

1) Increase in the safety from electricity dangers or risks
2) Increase in physical and cyber security
3) Better utilization of data or assets
4) Lower computational and maintenance cost
5) Electricity bill minimization
6) Disruption due to power quality issues should be minimize
7) A reduction of rate and length of outages

A. Data aggregation in smart grid

Data aggregation is clubbing of information from sensor nodes to an intermediate node also called aggregator. In smart grid systems if data aggregation can be done at AMI (Advanced metering Infrastructure) instead of utility centre then that system will be more efficient and secure. In aggregation operation data is collected from different sensor nodes or smart devices and this summation is based on specific variable performed on that data.

Wireless sensor network (WSN) formed by various numbers of wireless sensor nodes and a sink node or also called as base station. The base station is provided with unlimited available energy to be secure while the sensor nodes are provided with limited available energy therefore sensor nodes are unsecure. The sensor nodes observe an area associated with its HAN and collect the sensory information from it. This sensed information is transferred to sink node that is base station through wireless hop-by-hop communication. To preserve energy, sensed information is aggregated at intermediate sensor nodes or aggregators by applying a suitable aggregation function on that received data. Aggregation procedure minimizes the amount of network traffic that will help to reduce energy consumption on sensor nodes. Secure Data Aggregation in WSN is nothing but providing security while aggregation procedure. Fig 1 shows the data aggregation scenario in smart grid in which various smart meters are shown whose data combined at home area network using data collectors and this data then combined at building area network and finally combined at neighbourhood area network controller.

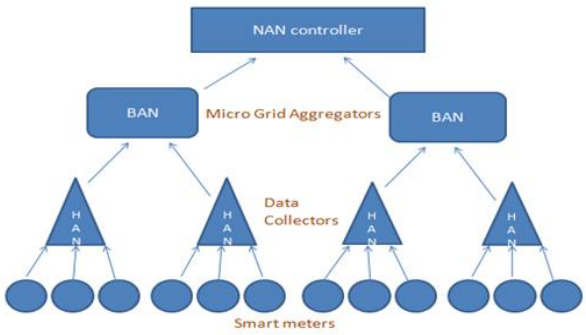

Figure 1: Data aggregation in smart grid

B. Security in smart grid

Smart grid system provides various security benefits that are privacy and integrity of collected data. Electricity usage is sensed and clubbed according to timely manner on a large scale. As sensing is passive, consumers have little awareness of their data exposure. Utility centre should have guarantee on integrity of data collected from Advanced metering infrastructure systems, as electricity fraud and attacks will prevented by accurate electricity information. Accuracy of collected data is important so as to provide correct billing information.

2. Related Work

Navid Alamatsaz, Arash Boustani, Murtuza Jadliwala, & Vinod Namboodiri et.al [1] has given coding theory and CDMA channel based technique in "AgSec: Secure and Efficient CDMA-based Aggregation for Smart Metering Systems" has proposed that to secure metering data, CDMA based data aggregation method provides access to all the data of all the smart meters in the root node(utility centre).This technique imposes lesser delay and overhead on SGNs as compared to cryptographic approaches and uses code division multiplexing to enable simultaneous transmission, reduce bit error rate and interference.

Xiaolei Dong, Jun Zhou, Khalid Alharbi, Xiaodong Lin, Zhenfu Cao et.al [2] has given privacy-preserving aggregation technique which uses elgamal encryption, which is secure under chosen plaintext attack. This technique can protect the user's meter reading data from sophisticated attacks sponsored by community gateway and users.

Muhammad Daniel Hafiz Abdullah, Ian Welch, Winston K. G. Seah et.al [3] has given hop-by-hop security approach in "Efficient and Secure Data Aggregation for Smart Metering Networks" that allows source and data integrity checks using pairwaise key and MAC to ensure source authenticity an data integrity against the impersonation and false data injection attacks.This technique eliminates the need to rely solely on the collector for verification process has been able to achieve low data loss and efficient attack detection.This technique has data confidentiality and privacy as a challenging task.

Haiyong Bao & Rongxing Lu et. al [4] has proposed data aggregation technique for achieving both differential privacy and fault tolerance in *"*DDPFT: Secure Data Aggregation Scheme with Differential Privacy and Fault Tolerance*"* which uses symmetric geometric distribution technique. The proposed data aggregation protocol is secure in a more challenging threaten model which covers communication attack, differential attack, and malware attack.

Mustafa A. Mustafa and Ning Zhang & Georgios Kalogridis and Zhong Fan et.al [5] has proposed a decentralized, efficient and selective aggregation (DESA) scheme for secure and privacy preserving communication in AMI. It is multi-recipient system model which uses the homomorphic Paillier cryptosystem to encrypt users' consumption data, which are aggregated by local gateways by selectively. DESA uses the BLS signature and batch verification methods to reduce operational and communicational overheads.

Min Lu, Zhiguo Shi, Rongxing Lu, Ruixue Sun, and Xuemin (Sherman) Shen et.al [6] has written "PPPA: A Practical Privacy-Preserving Aggregation Scheme for Smart Grid Communications" and proposed that PPPA technique utilizes the lightweight cryptographic aggregation technique to achieve deterministic security guarantee, uses the differential privacy technique to achieve privacy preservation of each individual user, and the quad tree structure to achieve failure tolerance.

Ruixue Sun, Zhiguo Shi, Rongxing Lu, Min Lu, and Xuemin (Sherman) Shen et.al [7] has described an efficient aggregation technique with error detection in "APED: An Efficient Aggregation Protocol with Error Detection for Smart Grid Communications" proposed protocol employs a pair wise private stream aggregation scheme to achieve privacy-preserving aggregation and perform error detection when some smart meters are malfunctioning.

3. Data Aggregation Approaches

There are various data aggregation approaches that are as given below.[8]

A. Tree Based Approach

In this approach tree structure formed first and then it is utilized later for routing of collected data according to the tree links. This approach combines the data at each level of tree and finally all the collected information is collected at root node. If the packet is lost in particular level in the tree due to various factors like channel destruction, noise then information present in complete structure of packet will get destroyed[8]. This approach is more useful while discovering efficient aggregation and to perform effective power utilization. In tree based approach various sensor nodes and base station shown as tree like structure. There are various leaf nodes and parent nodes in tree based structure. Leaf nodes data is combined into parent node of those particular nodes and again parent nodes data combined at root node that is base station or sink node. Fig 2 shows the tree based approach.

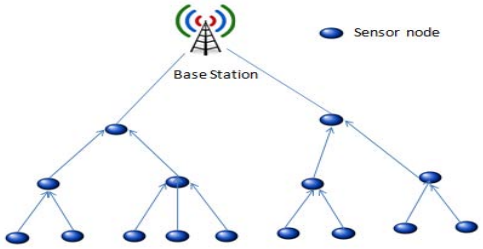

Figure 2: Tree based approach

B. Cluster Based Approach

This approach makes use of hierarchical structure of the network which combines various clusters data so as to send it to base station[8]. In this approach sensor nodes are partitioned into number of clusters. Certain nodes are selected so as to act like cluster-heads. Cluster head behave as aggregation node and they have direct communication with base station that is sink node. Fig 3 shows the cluster based approach.

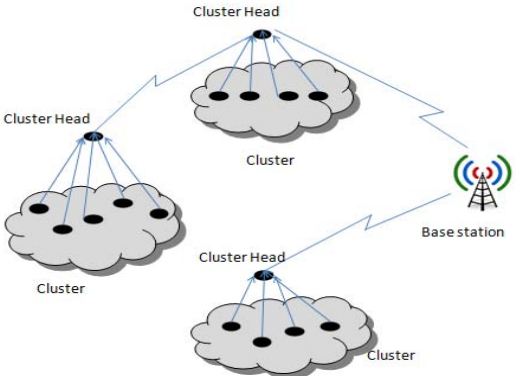

Figure 3: Cluster based approach

C. Structure-Less Approach

This approach is less important therefore not used in data aggregation. Particular structure is not formed in this approach therefore called as structure-less. Any cast mechanism is used for sending data packets to one hop neighbors which are having packets for aggregation purpose[8].

4. Methods for providing security

There are various methods available to provide security in data aggregation process. That are based on cryptographic techniques and chip code based techniques.

1. **Homomorphic encryption**
   Homomorphic encryption[3] is an encryption technique that allows performing computation on ciphertext thus generates encrypted results which when decrypted, matches the result of operation performed on plaintext. There are two types of homomorphic encryption techniques that are partially homomorphic encryption and fully homomorphic encryption. Homomorphic encryption would allow the different operations to be performed together in sequence without revealing the data of that service.
2. **Paillier cryptosystem**
   It is probabilistic asymmetric algorithm for public key cryptography, [9] Computation of n residue classes is computationally difficult. The assumption about decisional composite residuosity is the intractability hypothesis upon which this cryptosystem is based. The scheme is an additive homomorphic cryptosystem, this means addition operation on plain text will give the same output as multiplication over cipher text. If we know only public key and the encryption of m_1 and m_2, one can compute the encryption of $m_1 + m_2$.
3. **Bilinear pairing**
   Pairing-based cryptography will make use of pairing between two different cryptographic groups to map it with third cryptographic group as $e : G_1 \times G_2 \rightarrow G_T$ to construct or analyze cryptographic systems. Pairing can reduce hard problem in one group to different problem in another group, usually simple problem in another group. Pairings have been used to construct different cryptographic technique for which no other efficient implementation is not given, like as identity based encryption or attribute based encryption techniques.
4. **ElGamal cryptosystem**
   ElGamal encryption technique uses asymmetric keys for encryption and decryption[3]. It is public key cryptographic technique which is based on Diffie-Hellman key exchange problem. This technique of encryption can be defined over any cyclic group. Security of this technique depends upon the difficulty of discrete logarithmic operation. It is used in hybrid cryptosystem where message itself is encrypted using a symmetric cryptosystem and ElGamal is then used to encrypt the key used for the symmetric cryptosystem. ElGamal encryption is probabilistic in nature meaning that a single plaintext can be encrypted to many possible ciphertexts, therefore it is more secure because for one plaintext, different number of cipher texts are available.
5. **Orthogonal Chip code based technique**
   Hadamard matrix based on walsh function is very well-known choice than other chip code based methods[1][2]. This matrix is used to extract mutual orthogonal codes. Each row of hadamard matrix is taken as chip code. Dimension of the matrix depends upon the number of active smart devices available in HAN. Haramard matrix posses one property that, dot product of any pair of orthogonal chip codes is zero.

5. Comparison

Table: Comparison between various aggregation protocols

Title	Mechanism	Limitation
A secure data aggregation and dispatch scheme in smart grid[10]	Uses orthogonal chip code technique to achieve security.	Home power management is not done regarding to Privacy of customer power usage.
AgSec: Secure and efficient CDMA based aggregation[1]	Coding theory used for secure data aggregation. CDMA channel is used to aggregate data.	Not implemented in real test bed systems.
APED: An efficient aggregation protocol with error detection[7]	Uses pairwise private stream aggregation scheme. Handles user failure and detect malfunctioning of smart meters.	1) Privacy-preserving aggregation method needs to be more efficient. 2) Error detection mechanism needs to be more powerful.
Efficient and secure data aggregation for smart metering networks[3]	Provides early detection of impersonation and false data injection attacks. Uses hop-by-hop security mechanism. Pair wise key & message authentication code ensure authenticity & integrity.	1) More communication and computational overhead. 2) Transmission delay is more. 3) Data confidentiality and privacy is challenging task.
DDPFT: Secure Data Aggregation with Differential Privacy and Fault Tolerance [4]	By introducing auxiliary ciphertexts data aggregation can be achieved. Covers communication attack, differential attack, and malware attack.	Transmission time is more when user's number is less.
An ElGamal-Based Efficient and Privacy-Preserving Data Aggregation [2]	1) Uses Elgamal encryption which is secure under chosen plaintext attack. 2) Protects the user's meter reading data from sophisticated attacks encountered by community gateway and users.	Not secure under chosen ciphertext attack.
PPPA: A Practical Privacy-Preserving Aggregation[6]	1) Utilizes the lightweight cryptographic aggregation technique. 2) Data aggregation performed on ciphertexts at local gateway without decryption and results are reported by relays to the control centre.	1) Data pollution attack is not handled. 2) Internal attacks due to local gateways not handled.
DESA: Decentralized, Efficient and Selective Aggregation [6]	1) Uses a multi-recipient model and homomorphic paillier cryptosystem. 2) Adopts BLS signature and batch verification method.	Communication and computation overhead is more.

6. Conclusion

Security in smart grid data aggregation technique is new research area which is rapidly growing in latest technologies in various fields. We introduced data aggregation in smart grid systems and security requirements and also summarized network models to achieve efficient and secure information delivery in smart grid network. In home area network the smart grid system provides data aggregation techniques which need to be efficient and secure according to the applications purpose. We presented a comprehensive survey of network models and security techniques based on cryptographic approach and chip code approach for performing secure data aggregation in smart grid systems.

References

[1] Y. Ye, H. Sharif, Y. Yan, Y. Qian, and H. Sharif, "A Secure Data Aggregation and Dispatch Scheme for Home Area Networks in Smart Grid A Secure Data Aggregation and Dispatch Scheme for Home Area Networks in Smart Grid," 2011.
[2] N. Alamatsaz, A. Boustani, M. Jadliwala, and V. Namboodiri, "AgSec : Secure and Efficient CDMA-based Aggregation for Smart Metering Systems."
[3] X. Dong, J. Zhou, K. Alharbi, X. Lin, and Z. Cao, "An ElGamal-Based Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid," pp. 4720–4725, 2014.
[4] M. Daniel, H. Abdullah, I. Welch, and W. K. G. Seah, "Efficient and Secure Data Aggregation for Smart Metering Networks," pp. 71–76, 2013.
[5] H. Bao and R. Lu, "DDPFT : Secure Data Aggregation Scheme with Differential Privacy and Fault Tolerance," pp. 7240–7245, 2015.
[6] M. A. Mustafa and N. Zhang, "DESA : A Decentralized , Efficient and Selective Aggregation Scheme in AMI," pp. 0–4, 2014.
[7] M. Lu, Z. Shi, R. Lu, R. Sun, and X. S. Shen, "PPPA : A Practical Privacy-Preserving Aggregation Scheme for Smart Grid Communications," no. Iccc, pp. 692–697, 2013.
[8] R. Sun, Z. Shi, R. Lu, M. Lu, and X. S. Shen, "APED : An Efficient Aggregation Protocol with Error Detection for Smart Grid Communications," pp. 432–437, 2013.
[9] A. K. Talele, "A Survey on Data Routing and Aggregation Techniques for Wireless Sensor Networks," 2015.
[10] N. Saputro and K. Akkaya, "Performance Evaluation of Smart Grid Data Aggregation via Homomorphic Encryption," pp. 2972–2977, 2012.