Advances in Computer Science and Information Technology (ACSIT)
Print ISSN : 2393-9907; Online ISSN : 2393-9915; Volume 2, Number 7; April – June, 2015 pp 13 – 20
Krishi Sanskriti Publications
http://www.krishisanskriti.org/ACSIT.html

Secure Data Aggregation Using Homomorpic Encryption in Wireless Sensor Networks: A Survey

Sahira S. Maksud[1] and Ashish D. Patel[2]

[1,2]Department of Computer Engineering-IT Shri S'ad Vidya Mandal Institute of Technology Bharuch 392-001, Gujarat, India
E-mail: [1]sahiramaksud@gmail.com, [2]ashishpatel.svmit@gmail.com

Abstract—*Wireless Sensor Networks (WSNs) led to many new applications such as target tracking & habitat monitoring. However, large portion of total energy of WSNs is consumed due to Data communication between nodes. Data aggregation techniques greatly help to reduce energy consumption by eliminating redundant data. The security issues such as data confidentiality, data integrity & freshness in data aggregation is important when the WSN is deployed in remote & hostile environment where sensors having tendency of node failure and compromises. In this paper will survey these work and classify them in hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation. Also will discuss the security issues in data aggregation for WSN which will help us to identify and predict future of the sensor nodes with secure and energy efficient data aggregation.*

Keywords*: Wireless sensor networks, data aggregation homomorphic encryption, security, survey.*

1. INTRODUCTION

Wireless sensor networks (WSN) usually consist of hundreds and thousands of sensor nodes with limited power, computation, storage, sensing and communication resources [1]. Now sensors are becoming less expensive due to the advancement of technologies. Hence, it is a challenging task to provide efficient and effective solutions to data gathering problem. But the battery power is the most limiting factor in designing of wireless sensor network protocols which reduces power consumption by several mechanisms proposed such as radio scheduling, control packet elimination, topology control and data aggregation [2]. Generally, secure data aggregation uses two methods in WSN such as, hop-by-hop data aggregation and end-to-end data aggregation. Data aggregation main aim is to combine and summarized data packet of many sensor nodes so that amount of data transmission is reduced. In figure-1, example of data aggregation scheme is presented. Where group of sensor nodes collect information from target region [3]. Here, base station queries the network, instead of sending individual sensor node data to base station, one of the nodes called as data aggregator collects the information from its neighboring node, aggregate them and send the aggregated data to the base station over a multi-hop path.

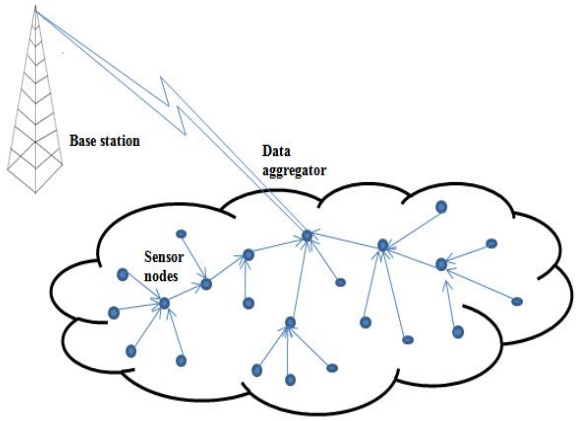

Fig. 1: Data aggregation in a wireless sensor networks

In wireless sensor networks, data aggregation operation improves the bandwidth and energy utilization, but it may also affect other performance metrics such as delay, fault tolerance, accuracy and security. In WSN, it is important to maintain certain level of security. It is not possible to sacrifice security for data aggregation. Also, there is a strong conflict between security and data aggregation protocols. Security protocols needs sensor node to encrypt and authenticate any sensed data prior to its transmission and prefer data to be decrypted by the base station [4]. While, data aggregation protocol prefer plain data to implement data aggregation at every intermediate node so that energy efficiency is increased. So it's a challenging task to provide source and data authentication along with data aggregation in WSN.

In this paper, we aim to provide an extensive overview of secure data aggregation concept in wireless sensor networks by defining the security requirements and issues and also we look at the data aggregation problem from the security perspective by giving comprehensive literature survey.

2. REQUIREMNETS OF DATA AGGREGATION SECUIRTY IN WSN

Most of the wireless sensor networks are deployed in remote and hostile environment and its challenging task to protect sensitive information transmitted by wireless sensor networks [5]. In this section, we have present essential security requirements that are raised in a WSNs environment for data aggregation process. In figure-2 it describes about security requirements and action with data aggregation process in wireless sensor network [3].

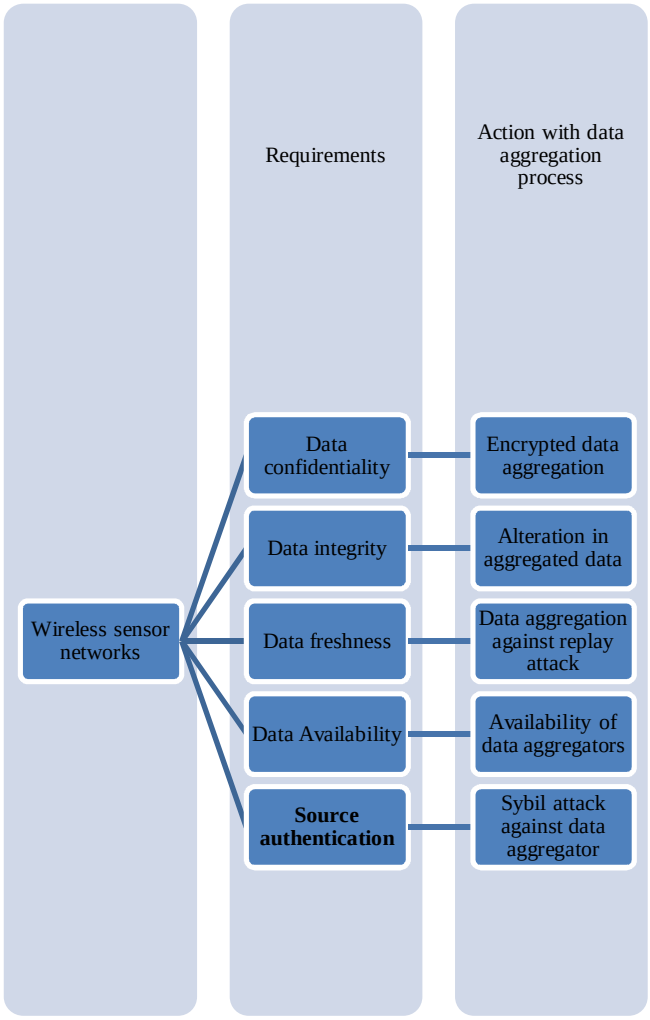

Fig. 2: WSN security for data aggregation

1. **Data confidentiality:** In WSN, data confidentiality ensure that information content is never disclosed to unauthorized parties and is most important issue for mission critical application. So, information should be sent in an encrypted form to provide secrecy. And this encryption should be done by the secret key such that intended party that has key can only open and read data [6].
2. **Data integrity:** Data integrity guarantees that a message being transmitted is never corrupted or tempered. As malicious node may just corrupt message to prevent network from the functioning [7].
3. **Data freshness:** It ensures that data are no old message which have been replayed but are the recent data which helps to protect data aggregation against replay attack and provide data freshness [7].
4. **Data availability:** Availability guarantees that network is alive and that data are accessible. It is strictly recommended in presence of compromised node to achieve network degradation by eliminating these bad nodes [3].
5. **Source authentication:** It allows a receiver to verify or confirm whether data is truly sent by claimed sender. The authentication mechanism is needed to detect maliciously injected and spoofed packet. Without source authentication an adversary could masquerade anode and hence gaining unauthorized access to the resources and sensitive information and it can perform operations to other nodes [6].

3. RELATED WORK

In this paper we survey different schemes for data aggregation using homomorphic encryption used in wireless sensor networks for preserving aggregation in WSNs.

Suat Ozdemir [8] proposed a protocol that achieves data aggregation and secures communication together. It is based on concealed data aggregation protocol to improve data aggregation, energy efficiency and bandwidth utilization. It imposed computation overhead by the privacy homomorphic encryption functions which are being employed by set of powerful nodes known as AGGNODES. Here, privacy homomorphic offers end-to-end concealment of data and ability to operate on cipher text. This scheme is feasible for the large heterogeneous wireless sensor networks.

A.S.Poornima et al. [9] proposed a secure data aggregation scheme which is based on secure end-to-end data privacy with the less number of bits transmitted for providing secure data aggregation. The protocol uses hop-by-hop feature for transmitting bits and end-to-end features for data privacy of the aggregated data. The data encrypted at SN-node is decrypted by the sink node on the aggregator nodes. The cipher texts are added and it uses additive homomorphic encryption for addition of cipher text which when decrypted result in addition of the plain text respectively.

The scheme proposed in [10] for data aggregation which employs elliptic curve cryptography based homomorphic encryption algorithm that offers data integrity and data confidentiality considering hierarchical data aggregation. Here it allows aggregation of data packet encrypted with different keys. During decryption of aggregated data the base station is able to classify the encrypted and aggregated data based on

encryption keys. Also, the proposed protocol provides integrity protection to aggregated data. The IPHCDA is compared with other public key-based homomorphic encryption schemes such as EC-OU and EC-EG.

Soufiene Ben Othman et al. [11] proposed an approach which uses homomorphic encryption EC-OU algorithm to achieve data confidentiality while allowing in-network aggregation along with additively digital signature algorithm based on ECDSA to achieve integrity of the aggregate in wireless sensor network. But still this approach is not worked for concealed data aggregation. With its performance evaluation the proposed scheme is efficient and feasible for the large wireless sensor networks.

Merad Boudia Omar Rafik et al. [12] proposed a fast and secure implementation of ECEG homomorphic encryption scheme on micaz mote. A fast scalar multiplication is employed which is also secure against the side channel attacks and it proves that SCA resistivity cost is not so important and it can achieve resource constrained motes. And also fast point decompression is used to allow aggregator for fast homomorphic operations to be done. Finally, it is concluded that asymmetric cryptography is feasible in wireless sensor networks by using ECC.

In [13] main focus is on the scalar point multiplication, its efficiency and the security against SCA in the context of Wireless sensor network. The most expensive operation in ECC is scalar point multiplication. The side channel attack (SCA) on ECC exploits the information leak during execution in order to find secret key. The result of the proposed work proves that cryptography is feasible in wireless sensor networks by using ECC.

The work in [14] provides both end-to-end confidentiality and end-to-end integrity with SA-SKPC, a secure data aggregation scheme for wireless sensor network (WSN) which is based on stateful public key encryption and homomorphic encryption. The proposed scheme is composed of two main phases such as, the forwarding phase and aggregation phase. Initially all sensor send their state which will be used in aggregation phase. While in later phase the sensor nodes encrypt and authenticate their captured data using the state shared with the base station present. Then the cluster head combines all cipher text and tag into one cipher text using homomorphic operation and X-OR operation. And finally, base station verifies the data which are aggregated and then decrypting the aggregate it retrieves the plaintext and verifies the integrity packet and authenticate sender.

In [15], the author proposed a new revised ElGamal and new homomorphism based on the new ElGamal. Also, new additive, multiplication and mixed multiplicative homomorphism based on HNE (NA-HNE, NM-HNE, NMM-HNE) are defined , so that it can work together to encrypt the arithmetic additive operation and multiplicative operation. Security analyses shows that HNE can resist the known-plaintext and chosen cipher-text attacks and enable to solve the problem of information leak.

In [16] provides efficient data aggregation while preserving data privacy. As it's a challenging task in wireless sensor network. They proposed two privacy preserving data aggregation schemes for additive aggregation functions such as, cluster based private data aggregation (CPDA) and Slice-Mix-AggRegaTe (SMART) which builds a slicing techniques focusing on additive data aggregation function.

In [17] proposed a privacy preserving K-mean clustering using Shamir secret sharing scheme in malicious adversary model. The two modifications to the local K-mean clustering algorithm depend on the distribution of data as an (1) horizontally partitioned data (2) vertically portioned data. This approach is efficient in terms of communication and computation cost. Also it supports malicious model using zero knowledge proof and verifiable secret sharing scheme. Additionally, we can explore the ECC based homomorphic public key cryptosystem to achieve privacy preservation in K-mean clustering.

In [18] authors proposed a family of secure perturbation-based schemes that can protect sensor data confidentiality without any disruption of additive data aggregation. In this schemes, the base station shares a secret with each sensor node. So that when a sensor node has a sensory data item to report, the original data are not reported but the sum of the original data and the secret shared with the base station. The scheme provides confidentiality protection for both raw and aggregated data with lower head compared to existing schemes

Merad Boudia Omar Rafik et al. [19] proposed a scheme robust and secure aggregation of encrypted data is based on an additive homomorphic encryption algorithm that allows integrity verification at intermediate node. It ensures the base station to receive ciphertexts which come from legitimate node and which also improves efficiency.

The author of [20] proposed the first secure data aggregation scheme based on elliptic curve cryptography, in this scheme data is encrypted hop-by-hop, and once received the cluster head computes the average and it sends result to its members. Also, each sensor compare the result with its own value and if the difference is more and beyond threshold, partial signature on average is performed for it and sent to CH. CH then combines all signature in one full signature and that result is forwarded to base station. But this scheme needs high communication costs to validate data and it supports average aggregation function.

The work in [21] provides both the end-to-end confidentiality and end-to-end integrity, they used ECEG and for integrity purpose they used aggregated signature scheme that are final verifier that has to know not only the individual data but also public key used for signature in order to verify the signature,

but problem in this function is that if number of nodes increase packet size increase.

In [22], the author proposed the end-to-end integrity with aggregate signature based on ECDSA using homomorphic encryption. That uses signature scheme without hash function to allow addition operation. The scheme leads to an important communication and computation overhead because packet contains ciphertext, public key and signature. This scheme can only verify the final aggregate so, when verification fails then important number of legitimate packet is lost.

In [23], proposed approach Enhanced Privacy Preserving Pattern-Code Based Data Aggregation (EPPCBDA) scheme in wireless sensor networks. That combines the strength of Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks (ESPDA) and Perturbation-based Efficient Confidentiality Preserving Protocol (PEC2P). By using pattern codes approach that will avoid energy waste because of sending redundant data to cluster heads and perturbation algorithm is more helpful in providing high data privacy and confidentiality.

4. CONCLUSION AND FUTURE SCOPE

In this paper, we provide a comprehensive overview of secure data aggregation concept in wireless sensor networks. Although presented research still addresses many problems for secure data aggregation, especially from the security point of view in wireless sensor networks. So, firstly the security requirements of wireless sensor network are presented with relationship between data aggregation concept. Secondly, an extensive survey of different schemes is studied comparatively for secure data aggregation in wireless sensor network. After the study of different aggregation techniques, pattern code based data aggregation technique is good for removing redundant data in WSNs. Also, combine features of homomorphic encryption Elliptic Curve Okamoto Uchiyama algorithm and Elliptic Curve digital signature algorithm techniques supports the security issues in data aggregation. According to this survey, the combine techniques of pattern code based data aggregation and combine features of homomorphic encryption Elliptic Curve Okamoto Uchiyama algorithm and Elliptic Curve digital signature algorithm achieves higher energy efficiency and security. We can conclude that this technique is more accurate than other data aggregation techniques. In future, a one data aggregation technique should be able to achieve energy efficiency and security accurately as per network parameters.

APPENDIX A: Table 1. Comparative study of different scheme for secure data aggregation in Wireless sensor networks

Title Name	Commentary	Issues Addressed	Methodology	Advantages	Limitations	Future Scope
Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism [8]	Is based on concealed data aggregation protocol. To improve data aggregation, energy efficiency and bandwidth utilization. Privacy homomorphism which offers end-to-end concealment of data and ability to operate on ciphertexts.	Data aggregation, energy efficiency and bandwidth utilization	Privacy homomorphic encryption algorithm in CDAP, only AGGNODEs are allowed to encrypt and aggregate the collected data using privacy homomorphic algorithm	Computation power and battery capacity	Disclose information of the neighboring data, inject false data May disclose	Is to reduce the computational overhead of privacy homomorphic encryption process by using field programmable gate arrays(FPGAs)
SEEDA: Secure End-to-End Data Aggregation in Wireless Sensor Networks [9]	Is based on secure end-to-end data privacy with less number of bits transmitted for providing secure data aggregation	Data transmission, End-to-End confidentiality	Secure end –to-end data aggregation scheme which provides end-to end privacy and additive homomorphic encryption to encrypt data	Reduces number of bit transmitted, network lifetime increases	Security issues are not fulfilled	We can reduce number of bits transmitted per node compared to other scheme

Integrity Protecting Hierarchical Concealed Data Aggregation For Wireless Sensor Networks [10]	Is based on a homomorphic encryption algorithm, and it allows the aggregation of the data packet encrypted with different keys. During decryption of aggregated data, the base station is able to classify the encrypted and aggregated data based on the encryption key.	Integrity, hierarchical data aggregation	Integrity protecting Hierarchical Concealed Data Aggregation protocol and scheme is based on elliptic curve cryptography based homomorphic encryption algorithm	Provides data confidentiality and integrity in multi data aggregator sensor network model	It is based on public key based homomorphic encryption schemes	IPHCDAs data aggregation should be compared with symmetric key based scheme
An Efficient Secure Data Aggregation Scheme For Wireless Sensor Networks [11]	Is based on homomorphic encryption while allowing in-network aggregation and uses additively digital signature algorithm based on ECDSA to achieve data confidentiality and integrity	Compromise attack, data confidentiality and integrity	It uses homomorphic encryption EC-OU to achieve data confidentiality and used additively digital signature algorithm based on ECDSA to a chive integrity	Helps to provide data confidentiality and data integrity	Redundant data are not eliminated	To implement the operation by eliminating redundant data
Fast and secure implementation of ECC- based concealed data aggregation in WSN [12]	Is based on ECEG homomorphic encryption which is efficiently implemented on MicaZ mote. From there result, it is been proved that cryptography is feasible in WSN by using ECC.	Need privacy and higher level of security	Implemented ECEG homomorphic scheme with fast scalar point multiplication and fast point decompression to reduce execution time and accelerate operation respectively	Helps to provide end-to-end data integrity and confidentiality	High overhead	In future algorithm needed for the implementation should be analyzed, selected and securely implemented
The impact of ECC's scalar multiplication on wireless sensor networks [13]	Is based on the efficiency and security of SPM in context of WSN. The side channel attacks (SCA) on ECC exploit the information leak during execution in order to find the secret key.	Scalar point multiplication, efficiency and security	ECC based scheme depends on the performance of Scalar point multiplication.	Helps to fulfill security needs.	To improve efficiency.	The aim is to implement SPM algorithm which not only prevent the side channel attack but helps to improve the efficiency.
SA-SPKC: Secure and efficient Aggregation scheme for wireless sensor networks using stateful public key cryptography [14]	The SA-SPKC a secure data aggregation scheme based on stateful public key encryption and homomorphic encryption	Data confidentiality and data integrity	In SA-SPKC it uses additive homomorphic encryption and aggregate MAC to provide end-to-end confidentiality and the end-to-end integrity	Helps to provide security for data aggregation and reduce computation overhead in WSN	It works on stateful public key cryptography	We aim to implement this solution on any platform

A New ElGamal-based Algebraic Homomorphism and Its Applications [15]	The new revised ELGamal and new homomorphism based on the new ElGamal. The evaluation of encrypted Polynomials shows the problems of leaks about skeleton and equal coefficient are solved completely.	Information leak	A new revised ElGamal and new homomorphism based on the new ElGamal (HNE) are proposed	Helps to find known-plaintext attacks and chosen-ciphertext attacks.	It is used for algebraic homomorphic applications	It can be further used in other applications
PDA: Privacy-preserving Data Aggregation in Wireless Sensor Networks [16]	Efficacy of privacy , communication overhead preservation, , and data aggregation Accuracy is compared with data aggregation Scheme TAG, where no data privacy is provided.	Data privacy	Cluster-based Private Data Aggregation (CPDA) and Slice-Mix-AggRegaTe (SMART) , for additive aggregation functions in WSNs.	Helps to reduce computation overhead	It only works for data privacy	Work includes to designing private preserving data aggregation schemes for general aggregation functions
Privacy Preserving Distributed K-Means Clustering in Malicious Model [17]	Is based on clustering tools of data mining and widely used K-Means clustering algorithm.	Malicious adversary model, computation and communication cost	Privacy preserving K-Means clustering using Shamir's secret sharing scheme	Efficient in computation and communication cost	Trusted third parties	Explore the ECC based homomorphic public key cryptosystem to achieve privacy preservation in K-Means clustering.
Confidentiality Protection for Distributed Sensor Data Aggregation [18]	Is based on family of secret perturbation-based schemes that can protect sensor data confidentiality without disrupting additive data aggregation.	Efficiency and security	A confidentiality Protection based on the idea of secret perturbation. Also, FSP, O-ASP and DASP to improve the communication performance	Provides confidentiality for raw and aggregated data	Data integrity	In future we can explore the work to improve security requirements of data aggregation
Rsaed: Robust And Secure Aggregation Of Encrypted Data In Wireless Sensor Networks [19]	Is based On an additive homomorphic encryption algorithm that allows aggregation on encrypted data.	Efficiency and data integrity	ECEG for end-to-end security with Respect to active attacks and RSAED to reduce the overhead at aggregator nodes.	Improves data integrity and efficiency	Not useful for other operations of elliptic curve	To improve the performance of elliptic curve operations of scheme SPM and the point decompression .
SecureDAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks [20]	Is based on protocol and hierarchical network structure for establishing cluster key in senor networks using elliptic curve cryptosystems	Bootstrapping Keys, security	Elliptic curve cryptography scheme is used for security and SecureDAV protocol for the correct aggregate readings	Helps to reduce energy consumption	Hop-by –hop encryption	Explore the work on ECC based homomorphic public key cryptosystem

An Efficient and Verifiable Concealed Data Aggregation Scheme in Wireless Sensor Networks [21]	Is based on scheme that not only aggregates ciphertexts but also signatures. And by verifying aggregated signature, data integrity of each plaintext can be guaranteed	Data integrity and confidentiality	combines Boneh et al.'s aggregate signature scheme and Mykletun et al.'s concealed data aggregation scheme	Provides end-to-end data integrity and confidentiality	Number of node increases packet size increases	To implement and explore the problem of packet size
Secure hierarchical data aggregation in wireless sensor networks [22]	Is based on homomorphic encryption and additive digital signatures to achieve confidentiality, integrity and availability for in network aggregation in WSN	Security	Homomorphic encryption algorithm and digital signature algorithm based on ECDSA is used	Provides confidentiality, integrity and availability	Only verify the final aggregate	Implementation of this algorithm for further analysis
Enhanced Privacy Preserving Pattern-Code Based Data Aggregation Protocol in Wireless Sensor Networks [23]	Evaluating advantages and weaknesses of Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks (ESPDA) and Perturbation-based Efficient Confidentiality Preserving Protocol (PEC2P)	Data privacy	Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks (ESPDA) and Perturbation-based Efficient Confidentiality Preserving Protocol (PEC2P) is combined	Higher energy efficiency and confidentiality	Symmetric cryptography is used	Considering redundancy Occurrence between sensors within different clusters

REFERENCES

[1] Sang, Yingpeng, Hong Shen, Yasushi Inoguchi, Yasuo Tan, and Naixue Xiong. "Secure data aggregation in wireless sensor networks: A survey." In Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on, pp. 315-320. IEEE, 2006.

[2] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." *Computer networks* 52, no. 12 (2008): 2292-2330.

[3] Ozdemir, Suat, and Yang Xiao. "Secure data aggregation in wireless sensor networks: A comprehensive overview." *Computer Networks* 53, no. 12 (2009): 2022-2037.

[4] Hu, Lingxuan, and David Evans. "Secure aggregation for wireless networks." InApplications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, pp. 384-391. IEEE, 2003.

[5] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "A survey on sensor networks." Communications magazine, IEEE 40, no. 8 (2002): 102-114.

[6] Alzaid, Hani, Ernest Foo, and Juan Gonzalez Nieto. "Secure data aggregation in wireless sensor network: a survey." In Proceedings of the sixth Australasian conference on Information security-Volume 81, pp. 93-105. Australian Computer Society, Inc., 2008.

[7] Jha, Mukesh Kumar, and T. P. Sharma. "Secure data aggregation in wireless sensor network: a survey." International Journal of Engineering Science and Technology 3, no. 3 (2011).

[8] Ozdemir, Suat. "Concealed data aggregation in heterogeneous sensor networks using privacy homomorphism." In Pervasive Services, IEEE International Conference on, pp. 165-168. IEEE, 2007.

[9] Poornima, A. S., and B. B. Amberker. "SEEDA: Secure end-to-end data aggregation in Wireless Sensor Networks." In Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On, pp. 1-5. IEEE, 2010.

[10] Ozdemir, Suat, and Yang Xiao. "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks." Computer Networks 55, no. 8 (2011): 1735-1746.

[11] Ben Othman, Soufiene, Hani Alzaid, Abdelbasset Trad, and Habib Youssef. "An efficient secure data aggregation scheme for wireless sensor networks." InInformation, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference on, pp. 1-4. IEEE, 2013.

[12] Rafik, Omar, Merad Boudia, and Feham Mohammed. "Fast and secure implementation of ECC-based concealed data aggregation in WSN." In Global Information Infrastructure Symposium, 2013, pp. 1-7. IEEE, 2013.

[13] Rafik, Merad Boudia Omar, and Feham Mohammed. "The impact of ECC's scalar multiplication on wireless sensor networks." In Programming and Systems (ISPS), 2013 11th International Symposium on, pp. 17-23. IEEE, 2013.

[14] Rafik, Merad Boudia Omar, and Feham Mohammed. "SA-SPKC: Secure and efficient Aggregation scheme for wireless sensor networks using Stateful Public Key Cryptography." In Programming and Systems (ISPS), 2013 11th International Symposium on, pp. 96-102. IEEE, 2013.

[15] Chen, Liang, Yong Xu, Weidong Fang, and Chengmin Gao. "A New ElGamal-Based Algebraic Homomorphism and Its Application." In Computing, Communication, Control, and Management, 2008. CCCM'08. ISECS International Colloquium on, vol. 1, pp. 643-648. IEEE, 2008.
[16] He, Wenbo, Xue Liu, Hoang Nguyen, Klara Nahrstedt, and Tarek Abdelzaher. "Pda: Privacy-preserving data aggregation in wireless sensor networks." InINFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, pp. 2045-2053. IEEE, 2007.
[17] Patel, Sankita, and Devesh C. Jinwala. "Privacy Preserving Distributed K-Means Clustering in Malicious Model." (2013).
[18] Feng, Taiming, Chuang Wang, Wensheng Zhang, and Lu Ruan. "Confidentiality protection for distributed sensor data aggregation." In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.
[19] Conti, Mauro, Lei Zhang, Sankardas Roy, Roberto Di Pietro, Sushil Jajodia, and Luigi Vincenzo Mancini. "Privacy-preserving robust data aggregation in wireless sensor networks." Security and Communication Networks 2, no. 2 (2009): 195-213.
[20] Mahimkar, Ajay, and Theodore S. Rappaport. "SecureDAV: A secure data aggregation and verification protocol for sensor networks." In Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE, vol. 4, pp. 2175-2179. IEEE, 2004.
[21] Sun, Hung-Min, Yue-Hsun Lin, Ying-Chu Hsiao, and Chien-Ming Chen. "An efficient and verifiable concealed data aggregation scheme in wireless sensor networks." In Embedded Software and Systems, 2008. ICESS'08. International Conference on, pp. 19-26. IEEE, 2008.
[22] Albath, Julia, and S. K. Madria. "Secure hierarchical data aggregation in wireless sensor networks." In Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE, pp. 1-6. IEEE, 2009.
[23] Ntirenganya, Bernard, Zijian Zhang, Liehuang Zhu, Yu-An Tan, Zhen Yang, and Cong Guo. "Enhanced Privacy Preserving Pattern-Code Based Data Aggregation in Wireless Sensor Networks." In Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on, pp. 336-341. IEEE, 2013.