I.J. Information Technology and Computer Science, **2014, 05, 28-35**
Published Online April 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.05.04

Asymmetric Concealed Data Aggregation Techniques in Wireless Sensor Networks: A Survey

Josna Jose
Assistant Professor, Dept. Computer Science and Engineering, Cochin University of Science and Technology, Kochi, India
E-mail: josnajose1990@gmail.com

Joyce Jose
Assistant Professor, Dept. Computer Science and Engineering, Cochin University of Science and Technology, Kochi, Kerala, India
E-mail: joycejose1990@gmail.com

***Abstract*—** The wireless communication nature of remotely deployed sensor nodes make the attacks more easily to be happened in wireless sensor networks (WSNs). But traditional security algorithms are infeasible in WSNs due to the limited computing, communication power, storage, band width and energy of sensor nodes. So energy efficient secure data aggregation schemes are necessary in resource constrained WSNs. Concealed Data Aggregation (CDA) based on privacy homomorphism (PH) gives a critical solution for energy efficient secure data aggregation in WSNs. PH based algorithms allow aggregation to be happened on cipher texts. Thus, it eliminates the power consuming decryption operations at the aggregator node for the data aggregation and further encryption for the secure transmission of aggregated data. It also avoids the aggregator node from the burden of keeping the secret key information and thereby it achieves energy efficiency and reduces the frequency of node compromise attacks in aggregator nodes. Among the CDA techniques, asymmetric PH based CDA techniques are exploring due to their combination with elliptic curve cryptography having reduced key size. We present an overview of asymmetric concealed data aggregation techniques that achieve both end to end data confidentiality and non delayed data aggregation.

***Index Terms*—** Wireless Sensor Network, Data Aggregation, Secure Data Aggregation, Concealed Data Aggregation, End to End Encrypted Data Aggregation, Privacy Homomorphism

I. Introduction

Wireless sensor network consists of large number of physically deployed, low cost and small sized sensor nodes, which gathers sensing data from the physical environment and pass the sensed data to base station (BS) for further processing. Sensors are resource constrained in battery power, memory, communication and computation capabilities. Sensors have many applications in military field surveillance, health care, environmental monitoring, accident reporting and law enforcement.

Due to the dense deployment of sensor nodes, the neighboring sensor nodes often have overlapping sensing ranges and it produces some similar sensing data. Transmission takes more power in WSNs, so transmitting these redundant data is not efficient in energy constrained wireless sensor networks. The data aggregation [1], [2] technique which avoids the redundant data by aggregating the data coming from different sensor nodes using the aggregation functions such as MAX, MIN, Average etc and provides energy efficient solution for WSNs. The aggregated data transfer provides robust and accurate data at the BS by achieving band width and energy efficiency.

Data aggregation protocols [3], [4] are divided into tree based data aggregation protocols and cluster based data aggregation protocols based mainly on the topology used for data aggregation. Cluster based data aggregation protocols reduces the latency in the tree-based data aggregation by grouping the nodes in WSNs into clusters. This process is called clustering. In cluster based protocols, cluster head performs data aggregation and parent nodes in the path to the base station perform data aggregation in tree based data aggregation protocols.

The sensor nodes are usually deployed in hostile or unattended area which increases the chance of attack [25] in WSNs. Each aggregated result in WSNs have great effect in final aggregation result received from the BS because each aggregated result represents the data’s of many sensor nodes. So it is necessary to consider security along with data aggregation. Secure data aggregation protocols [4], [5], [6], [8], [9], [10], [11],

[12], [13], [14], [27], [28] tries to achieves security requirements [4], [6] such as data integrity, data confidentiality, data authentication, data freshness etc along with data aggregation. But hop by hop encrypted data aggregation protocols [4], [27] cause energy wastage at aggregator nodes due to the decryption and encryption operations at aggregator nodes for the data aggregation and further secure transmission respectively. The decryption of data's in the aggregator nodes increases the node compromise attack in aggregator nodes and it causes the revealing of large amount of information as well as the secret key to the adversary easily by losing the end to end confidentiality of data. So hop by hop encrypted data aggregation protocols does not provides critical solution for energy constrained security critical WSNs. The concealed data aggregation (CDA) techniques (End to End encrypted data aggregation) [26] allows aggregation on cipher text due to the privacy homomorphism (PH) property allows aggregation on encrypted data rather than plain sensor data and provides energy efficient secure data aggregation solution to WSNs. Among them, asymmetric PH based CDA techniques are important due to their support of elliptic curve cryptography having reduced key size (160 bit).Thus it provides better system security with reduced key size. So it is applicable for real time application requiring better security.

Rest of the paper is organized as follows. Section II describes concealed data aggregation. In section III, provides the details of existing asymmetric PH based CDA techniques. In section IV, we compare different asymmetric PH based CDA scheme based on some security factors along with other factors. Sections V discuss the current exploiting issues and future directions. Section VI concludes the work.

II. Concealed Data Aggregation

It is one of the secure data aggregation techniques that guarantee the in-network processing on encrypted data [7] and it achieves energy efficiency and secure communication together. The cryptographic algorithms that support privacy homomorphism are the foundation of CDA, which allows aggregation on cipher texts. The in network aggregation on encrypted data, aggregate the encrypted data close to the source node instead of transmitting the individual encrypted data through the entire networks. So it provides energy efficient secure data transmission by guaranteeing end to end confidentiality of sensor data's.

In Concealed data aggregation protocols (End to End encrypted data aggregation protocols) [8], [9], [10], [11], [12], [13], [14] the aggregators aggregate the encrypted sensor readings without decrypting them. So it saves the energy spend for decryption and encryption operations at the intermediate aggregator nodes. In CDA, Intermediate aggregator nodes need not want to store secret information hence it provides end to end privacy between sensor nodes and sink. CDA provides secure data aggregation without delay.

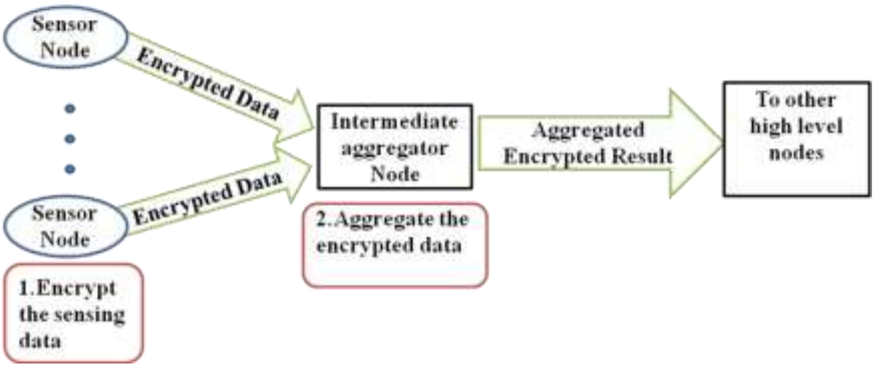
Sensor Node
Encrypted Data
Sensor Node
Encrypted Data
1.Encrypt the sensing data
Intermediate aggregator Node
2.Aggregate the encrypted data
Aggregated Encrypted Result
To other high level nodes

Fig. 1: Concealed Data Aggregation

2.1 Benefits of CDA

1) Reduced network traffic

Due to the in-network data aggregation support of CDA, data's are aggregated as close to the source node instead of transmitting to the BS directly. So CDA avoids the transfer of redundant data from the sensor nodes and achieves efficient network traffic.

2) Achieves end to end confidentiality of data

CDA based on privacy homomorphism supports aggregation on cipher text, so there is no need of performing decryption and encryption on aggregator nodes. Thus the sensor data's are concealed from the aggregator node and the sink node can only decrypt the aggregated data.

3) Reduced Energy Consumption

The privacy homomorphism allows aggregation over cipher texts. So CDA frees out the intermediate aggregator node from the energy consuming encryption and decryption operations. This leads to the reduced energy consumption at the intermediate nodes.

4) Low Memory consumption at intermediate aggregator nodes

There is no need of keeping secret information on intermediate aggregators in CDA. So it protects the aggregator nodes from the node compromise attack and reduces the memory needed for storing keys and dates for aggregation.

5) Reduced overhead at aggregator node

In CDA, intermediate aggregator nodes do not want to perform costly decryption and encryption operations at aggregator node. so aggregator nodes do not want to keep sensitive cryptographic key.

6) Improved Security

Adversaries are unable to gather information from transmission because data's are in encrypted form during the transmission. CDA provides probabilistic security as it reduces the chance of adversaries to catch the unencrypted data as aggregation is performed on encrypted data. So corrupted aggregator node could not know aggregation result.

7) Increased flexibility in changing routes

In hop by hop data aggregation, nodes which have keys can only decrypt the data and perform data aggregation. But in CDA every node can take the role of aggregator because there is no need of decryption at the aggregator node for data aggregation. So aggregator selection is based on remaining energy.

8) Reduced latency in network

Privacy homomorphism property of CDA supports aggregation directly on encrypted dates. This avoids the time spend for decryptions and encryption at the intermediate nodes. So it achieves data aggregation without delay and correspondingly reduces the packet dropping.

2.2 Privacy Homomorphism (PH)

It is an encryption transformation that allows direct computation on encrypted data's. Privacy homomorphic cryptography achieves both end to end confidentiality and data aggregation. Additive PH and multiplicative PH are the two variations of privacy homomorphism.

If an encryption algorithm E() is said to be additive homomorphic, then it support additive operations on encrypted data without the decryption of individual data's. ie. E(x+y) =E(x) +E(y).It is more suitable in wireless sensor network due to their less expensive operation than multiplicative PH.

If an encryption algorithm E() is said to be multiplicative homomorphic, then it support multiplicative operations on encrypted data without the decryption of individual data's. ie. E(x*y) =E(x) *E(y).

Cryptographic algorithms that support privacy homomorphism are divided into two. These are Symmetric PH [10], [28] and Asymmetric PH/ public key homomorphism.

1) Symmetric PH

In symmetric PH, node encrypts their sensor reading by the key shared to the base station. So the base station can only decrypt the data and can achieve end to end confidentiality. But security threats are more in sensor nodes due to the usage of secret keys in them.

2) Asymmetric PH

In asymmetric PH, nodes encrypt the sensing data with base station public key. So the base station owns the private key that can decrypt the data .So it achieves end to end confidentiality with minimum security threats to the sensor nodes. If an encryption transformation is said to be asymmetric additive PH, then it satisfy $a+b=D_r(E_u(a)+ E_u(b))$. If an encryption transformation is said to be asymmetric multiplicative PH, then it satisfy $a*b=D_r(E_u(a)* E_u(b))$.where (r,u) are public and private key pair.

Table 1: Difference between Symmetric PH and Asymmetric PH

Parameters	Symmetric PH	Asymmetric PH
Encryption and Decryption	using same key	using different key
Number of key	Single key	Multiple key
Key Management	More overhead	Less overhead
Aggregation Speed	Fast	Slow
Computational overhead	Low	Higher
Expensive	Less	more
Message size	Small	Large
Key size	Short	Long
Type of key stored by sensor node	Sensor node needs to store secret key	Sensor node needs to store non sensitive public key
Overall system security	Less	Better
Chosen plain text attacks	Insecure	Secure
Node compromise attack	Largely affected	Less affected
Example	Domingo-Ferrer [23],CMT[10]	EC-ElGamal [18],[16], EC-OU[19]

An efficient public key based PH [16] would be advantageous to easily prone resource constrained WSN. Because in asymmetric PH based CDA, node wants to store the non sensitive public key, and private key is kept in tamper resistant BS. But one of the important drawbacks is the large key size. Elliptic curve based asymmetric privacy homomorphism give relief to these by giving same security level as other asymmetric PH with smaller key size and cipher text. It reduces transmission overhead by small size of data packets.ECC based privacy homomorphism is preferable in resource constrained WSN.

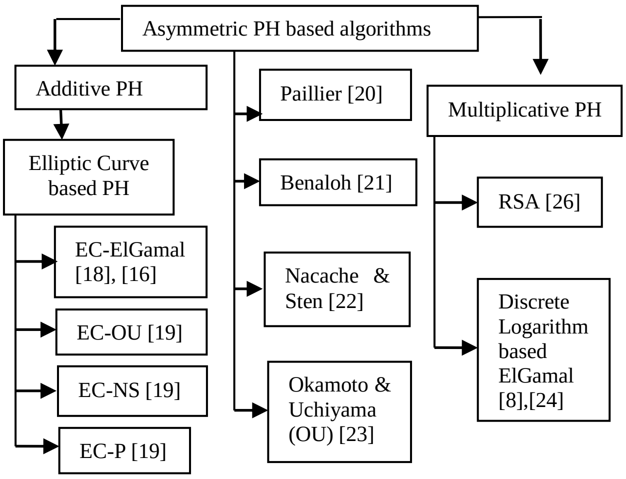

Fig. 2: Classification of asymmetric homomorphic encryption algorithms

2.3 Major attacks on CDA Scheme

1) Passive attacks

In this type of attacks, adversary listens the transmitted packets without actively interfering in the connection and then crypt analyze the eavesdropped information to obtain secret information. Preventing the gain of transmitted information with simple eavesdropping is the security goal of the prevention mechanism. The passive attack does not change the content of the transmitted packet.

a) Cipher text analysis

In this type of attack, an adversary tries to intercept the cipher text and then performs the analysis of encrypted packets to obtain secret information such as plain text and keys. The cryptographic system that prevents this attack must ensure that adversary is not able to decide whether an encrypted packet corresponds to specific plain text or not and prevent the gain of any sensitive information (key, plain text).

b) Known plaintext attack

This is one among the attacks in WSNs, where adversaries try to find out the secret information with the additional knowledge of plain text for deducting malicious cipher text or decrypting other messages with known plain text and corresponding cipher text. The adversaries can obtain the plain texts corresponding to the cipher text by guessing and manipulating the sensor readings or physically by capturing the deployed sensor nodes. The cryptographic algorithm that prevents the known plain text attack must prevents the deduction of secret keys or additional cipher text or plain text out of known set, even when large set of corresponding plain-cipher texts are available.

2) Active attacks

CDA techniques are more vulnerable to this attack in which adversaries can interfere the communication (catch, analyze, modify, replace & send packet). A successful active attack can lead to the destruction of whole network.

a) Reply attack

It is the resending of previously sent valid packet in wrong time to make malicious effects. Time stamp, inclusion of unique information from the previous transaction can be used as counter measures.

b) Malleability

This attack manipulates the content of valid encrypted packet without leaving scratch. This attack is possible in EC-EG and EC-EU by adding multiples of the generator point.

c) Forge attacks

It is one of the may attacks which can easily happen in asymmetric PH based CDA as sensor data is encrypted with base station BS public key. So adversary can create proper forged cipher text and substitute it with the actual cipher text. Cryptographic method prevents this attack by denying a third party to create a properly encoded cipher text. Digital signature can be used as preventive measure.

d) Unauthorized Aggregation

It is one of the main weaknesses of PH based algorithms in which adversary tries to compromise aggregator node and maliciously aggregates the cipher text and thereby generates bad but valid aggregated result. The cryptographic algorithm that prevents the attack can select a secret key for aggregation as counter measure so that the adversary cannot perform aggregation without knowing the key. As a counter measure, ensures that a cipher text cannot be used more than once so that the unauthorized aggregation can be detected by decryption unit.

3) Physical attacks

The deployment of sensor nodes in hostile or unattended area makes this attack easy on WSNs and it affects the hardware parts of the sensor nodes such as flash memory and reveals key information which destroys sensors permanently. This attack is more in symmetric encryption scheme that uses same key information on each node.

Table 2: Attacks on Asymmetric PH based algorithms(S-Secure V-Vulnerable)

Type of PH	**PH based algorithm**	**Passive attack**		**Active attack**				**Physical attack**
		Cipher text analysis	**Known plain text attack**	**Replay attack**	**Malle-ability**	**Unauthorized aggregation**	**Forge attack**	
Asymmetric PH	EC ElGamal [18][16]	S (++)	S (++)	V (--)	V (--)	V (--)	V (--)	S (++)
	EC-OU [19]	S (++)	S (++)	V (--)	V (--)	V (--)	V (--)	S (++)

III. Asymmetric PH based CDA Techniques

Asymmetric PH based CDA technique uses public private key management scheme in which the public key used for the encryption of sensing data and decrypting the data in BS. This type of CDA technique is crucial in security critical applications.

3.1 CDAP

Concealed Data Aggregation using Privacy Homomorphism [9] overcomes the computational overhead imposed by the asymmetric PH by a group of special sensor nodes called AGGNODEs. AGGNODEs have more memory, computational and battery power. In CDAP, firstly AGGNODEs receives the BS's public key and then network is deployed. After that, AGGNODEs establishes a pair wise secret key with neighboring sensor nodes using any of the random key distribution protocol. Then each sensor node encrypts their data using symmetric key encryption algorithm (RC5) as respond to the query received from the AGGNODEs in data collection phase. The use of symmetric key algorithm for encryption of sensor data may leads to the disclosure of secrecy of the neighboring nodes when the AGGNODEs became compromised. But this attack has local effect. The AGGNODEs decrypts all the received data's, aggregate them and encrypts the aggregated result using the public key of BS and send it to BS. So BS owns the private key that can decrypt the aggregation result. Thus the aggregated result is concealed from the nodes in the path to the sink. Through the path to the sink node, aggregated data are aggregated hierarchically and finally reaches the BS. At the sink node, the aggregated result is decrypted using BS's private key.

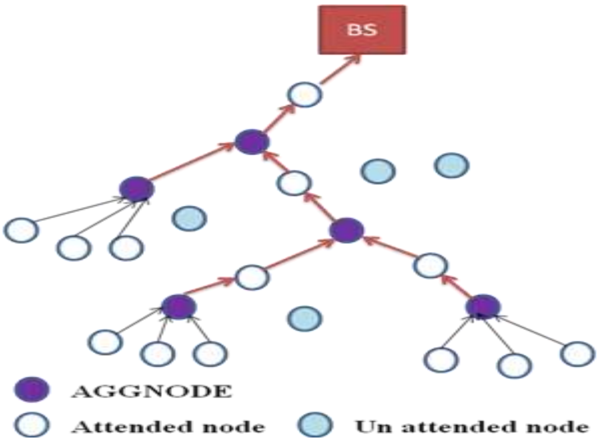

Fig. 3: Operation of CDAP protocol

CDAP have more computational overhead than hop by hop due to the asymmetric privacy homomorphism. But it achieves more data transmission efficiency and aggregation ability than hop by hop scheme if the number of AGGNODEs is more.

3.2 HCDA

Hierarchical Concealed Data Aggregation for Wireless Sensor Network [11] is based on the elliptic curve cryptography. So it is resistant to node compromise attack. This protocol provides concealed data aggregation by aggregating data of multiple sensor node group that use different public keys to encrypt their data. This is achieved by the help of group based network deployment scheme. In this, sensor nodes are divided into several groups before deployment and each group is deployed from certain location over the network, so that each group covers a part of the network. Then assign different public key to each group so that the BS is able to determine and classify the data of the group, based on the public key used to encrypt the data. This helps the base station to identify data of a particular region or group of networks. The members of a particular group encrypt their data with public key which is assigned to that group. In the group aggregator node, the data coming from the group members are aggregated without decryption. Then it passes this aggregated value to higher level aggregators to aggregate with other group aggregate. This procedure is repeated until the aggregated value reaches the base station.

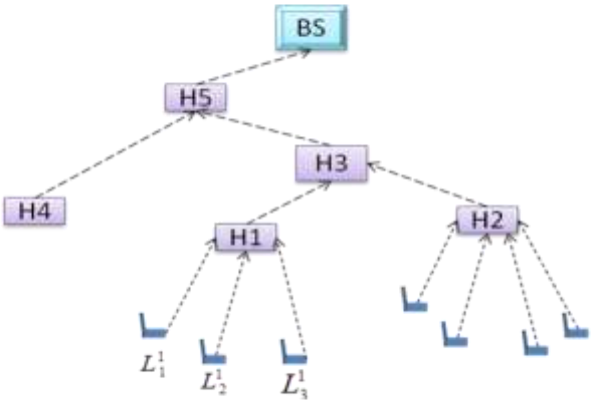

Fig. 4: Example of RCDA-HETE Network

IV. Comparison of Asymmetric Concealed Data Aggregation Techniques

4.1 Data Integrity

This security requirement provides the assurance to sink node that message has not been altered by malicious nodes during transmission. Alteration in aggregated data leads to the loss of data integrity in data aggregation process. Digital signature is commonly used in asymmetric cryptography for integrity checking.

4.2 Data Authentication

It ensures that the communicating node is the one that it claims to be. Sensor node uses shared wireless medium for communication. So source authentication is necessary in WSNs to identify maliciously injected or spoofed packets, in order to ensure that the data is from authorized one. The absence of authentication in data aggregation helps the attacker to claim that it is a legal one and can alter the aggregation result by providing false data. It prevents Sybil attack against aggregators and node impersonation.

4.3 Data Confidentiality

This security requirement keeps the sensitive transmitted information from unauthorized entities, so that the intended node can only read the data. End to end confidentiality can be achieved by the aggregation of encrypted data.

4.4 Aggregation function

It indicates those mathematical calculations that can be performed on sensor data.PH based algorithms only support limited number of aggregation functions. The RCDA [14] overcomes this limitation by recovering individual sensor readings at the BS.

4.5 Algebraic property of PH

This factor indicates the algebraic property of PH which is used in the asymmetric concealed data aggregation technique. Asymmetric PH based algorithms support additive and multiplicative homomorphic property. Addition and multiplication operations on encrypted data are supported by additive and multiplicative PH based algorithms respectively.

Table 3: Comparison of Different Asymmetric Concealed Data Aggregation Techniques

Asymmetric PH based CDA techniques	Data integrity	Data authentication	Data confidentiality	Aggregation function	Algebraic property of PH
CDAP[9]	No	No	Yes	Sum, Average, variance	Additive
HCDA[11]	No	No	Yes	Sum, Average, variance	Additive
SHCDA [12]	Yes	No	Yes	Sum, Average, variance	Additive
NSDA[13]	Yes	No	Yes	Sum, Average, variance	Additive
RCDA[14]	Yes	Yes	Yes	Sum, Average, variance, Maximum, Minimum	Additive

V. Current Exploiting Issues and Future Directions

The presented research paper addresses many problems of asymmetric concealed data aggregation. There are still many areas to explore deeply, especially in security point of view.

Some of the asymmetric concealed data aggregation only achieves data integrity and source authentication. It needs to be considered in every technique to guarantee the correctness of the data and the source of the data respectively. Because the sensor nodes uses wireless medium for communication, so attacker can gain access to the transmitted packet by simply tuning to the corresponding radio frequency. Aggregated signature scheme can be used to achieve data integrity and authentication. It needs to be explored deeply to provide guaranteed system with reduced energy. One of the crucial problems to be explored in the current exploiting asymmetric CDA is the detection of compromised nodes including aggregator node. The compromised nodes can change the aggregated result. Still there is no effective mechanism for it.

Elliptic curve based PH techniques are the exploiting area’s in resource constrained WSN due to their smaller key size with high security. But it supports only some aggregation function such as sum, average etc. So designing an efficient elliptic curve based PH that support all aggregation functions are need to be explored more in future research. Extending single level asymmetric PH based data aggregation into multilevel hierarchical data aggregation is the one of the research problem for the energy constrained WSN containing large number of sensor nodes. Use of the heterogeneity of nodes in wireless sensor network is another area for research.

VI. Conclusion

We present before you the important asymmetric concealed data aggregation techniques in WSNs. Asymmetric concealed data aggregation is a powerful solution for security needed wireless sensor networks due to the support of elliptic curve cryptography which provides high security with reduced key size. So it provides a highly secure and energy efficient solution for WSNs. Elliptic curve based PH provides solution for real time response applications that requires security. Asymmetric PH based techniques protect the aggregator node from the compromise of the attacker and provides relief to the node from the keeping of sensitive private key by providing real time data aggregation.

References

[1] Kiran Maraiya, Kamal Kant, Nitin Gupta. Wireless Sensor Network: A Review on Data Aggregation. International Journal of Scientific & Engineering Research, Vol. 2, Issue 4, April -2011, ISSN 2229-5518.

[2] Nandini. S. Patil, Prof. P. R. Patil. Data Aggregation in Wireless Sensor Network. IEEE International Conference on Computational Intelligence and Computing Research, 2010.

[3] P.D.Patel, Porf.P.B. Lapsiwala and R.V.Kshirsagar. Data Aggregation in Wireless Sensor Network, International Journal of Management, IT and Engineering, Vol. 2, Issue 7, July 2012, ISSN: 2249-0558.

[4] S.Ozdemir, Y.Xiao. Secure data aggregation in wireless sensor networks: A comprehensive overview. Computer Networks,Vol. 53, 2009, 2022–2037.

[5] Y.Sang and H Shen, Secure Data Aggregation in Wireless Sensor Networks: A Survey. Proc. IEEE Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT '06), December 2006, pp.315-320.

[6] Mukesh Kumar Jha,T.P. Sharma. Secure Data aggregation in Wireless Sensor Network: A Survey. International Journal of Engineering Science and Technology, Vol. 3, No. 3 March 2011, ISSN: 0975-5462.

[7] D.Westhoff,J.Girao and A.Sarma. Security Solutions for Wireless Sensor Networks. NEC TECHNICAL JOURNAL, Vol.1, No.3, 2006.

[8] Gwoboa Horng, Chien-Lung Wang, Tzung-Her Chen. "An Efficient Concealed Data Aggregation Scheme for Wireless Sensor Networks". Information Security and Cryptology Conference (ISCTurkey 2007), Ankara, Turkey, Dec. 13-14, 2007.

[9] S. Ozdemir. Concealed Data Aggregation in Heterogeneous Sensor Networks Using Privacy Homomorphism. Proc. IEEE Int'l Conf. Pervasive Services, July 2007, pp. 165-168.

[10] C. Castelluccia, E. Mykletun, and G. Tsudik. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks. Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems, July 2005, pp. 109-117.

[11] Suat Ozdemir and Yang Xiao. Hierarchical concealed data aggregation for wireless sensor networks. In: Proceedings of the Embedded Systems and Communications Security Workshop in conjunction with IEEE (SRDS 2009), 2009.

[12] Julia Albath and Sanjay Madria. Secure hierarchical data aggregation in wireless sensor networks. In: Proceedings of the, IEEE conference on Wireless Communications and Networking(WCNC 2009), 2009.

[13] Vivaksha Jariwala and Devesh Jinwala, A NOVEL APPROACH FOR SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS. 10th National Workshop on Cryptology, Department of Mathematics and Computer Applications, PSG College of Technology, Peelamedu, Coimbatore, September 2 – 4, 2010.

[14] Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun. RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 4, APRIL 2012.

[15] Hung-Min Sun, Chien-Ming Chen, Yue-Hsun Lin, and Ya-Ching Lin. Supplementary Material: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks. SUPPLEMENTAL MATERIAL FOR THE IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, *available on* http://doi.ieeecomputersociety.org/10.1109/TPDS. 2011.219.

[16] E. Mykletun, J. Girao, and D. Westhoff. Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks. Proc. IEEE Int'l Conf. Comm., vol. 5, June 2006, pp. 2288-2295.

[17] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), 2003, pp. 416-432.

[18] O.Ugus, A.Hessler, D.Westhoff. "Performance of Additive Homomorphic EC-ElGamal Encryption for TinyPEDS". Technical Report, 6, Fachgesprach "Drahtlose Sensornetze", July 2007, http://www.ist-ubisecsens.org/publications/EcElGamal-UgHesWest.pdf.

[19] P. Paillier. Trapdooring Discrete Logarithms on Elliptic Curves over Rings. Proc. Ann. Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT '00), 2000, pp. 573-584.

[20] P. Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '99), 1999, pp. 223-238.

[21] J. Benaloh. Dense Probabilistic Encryption, Proc. Workshop Selected Areas of Cryptography (SAC '94), pp. 120-128, 1994.

[22] D. Naccache and J. Stern. A New Public Key Cryptosystem Based on Higher Residues. Proc. ACM Conf. Computer and Comm. Security (CCS '98), 1998, pp. 59-66.

[23] T. Okamoto and S. Uchiyama. A New Public-Key

Cryptosystem as Secure as Factoring. Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT ’98), 1998, pp. 308-318.

[24] T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Proc. Ann. Int’l Cryptology Conf. (CRYPTO ’85), vol. 31, no. 4, July 1985, pp. 469-472.

[25] Dr.G.Padmavathi, Mrs.D.Shanmugapriya. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. International Journal of Computer Science and Information Security, Vol. 4,No. 1&2, 2009.

[26] S. Peter, D. Westhoff, and C. Castelluccia. A Survey on the Encryption of Convergecast-Traffic with In-Network Processing. IEEE Transactions on Dependable and Secure Computing, vol. 7,No.1, Januvary-March,2010.

[27] Josna Jose, Joyce Jose and Fijo Jose. A Survey on Secure Data Aggregation Protocols in Wireless Sensor Networks. International Journal of Computer Applications (0975 – 8887), Volume 55,No.18, October 2012.

[28] D. Westhoff, J. Girao, and M. Acharya. Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation, IEEE Trans. Mobile Computing, vol. 5, no. 10, Oct. 2006pp. 1417-1431.

Authors’ Profiles

Josna Jose: Received the Master of Technology (M Tech) in Network and Internet Engineering from karunya University, Coimbatore, Tamilnadu, India in the year 2013 and Bachelor of Technology (B Tech) degree in Computer Science & Engineering from Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India in the year 2011. She is working as Assistant Professor in the Department of Computer Science and Engineering, College of Engineering Cherthala under the Cochin University of Science and Technology, Kerala, India. She has published 3 International Journals and 2 International IEEE Conference papers. Her research interest is in the area of secure data aggregation in Wireless Sensor Networks.

Joyce Jose: Received the Master of Technology (M Tech) in Network and Internet Engineering from karunya University, Coimbatore, Tamilnadu, India in 2013 and Bachelor of Technology (B Tech) degree in Computer Science & Engineering from Viswajyothi College of Engineering & Technology, Vazhakulam, Kerala, India in the year 2011. She is working as Assistant Professor in the Department of Computer Science and Engineering, College of Engineering Cherthala under Cochin University of Science and Technology, Kerala, India. She has published 3 International Journals and 2 International IEEE Conference papers. Her research interest is in the area of privacy preserving data aggregation in Wireless Sensor Networks.

How to cite this paper: Josna Jose, Joyce Jose,"Asymmetric Concealed Data Aggregation Techniques in Wireless Sensor Networks: A Survey", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.5, pp.28-35, 2014. DOI: 10.5815/ijitcs.2014.05.04