Secure Data Aggregation Using RSA Algorithm

Mrs. Jyothi R[1], Dr.Nagaraj G Cholli[2]

Assistant Professor[1], Associate Professor[2]
Department of CSE[1],
Department of ISE[2],
GAT,Bangalore[1]
RVCE[2], Bangalore, India

***Abstract*--Wireless sensor networks are collection of sensor nodes and sink node, where sensor node performs sensing of data and communicating it with sink node and sink node is also called as base station, which receives sensed data from sensor nodes through cluster head in a network. This type of traditional method consumes more energy, which reduces the network lifetime because sensor nodes are battery powered. Data aggregation technique consumes less energy and eliminates redundant data in network. One more challenge in wireless sensor network is security. To prevent information from attackers and to keep information safe, a suitable cryptographic algorithm should be selected. In NS2, performance of RSA algorithm is evaluated and results of it shows RSA algorithm enhances both energy and security levels.**

Keywords: Cryptographic algorithm, RSA, Data aggregation, Wireless sensor network, Cluster.

1. Introduction

Wireless sensor networks consist of small sized low cost sensor nodes, the data in the environment are sensed and communicates the data gathered with sink node through wireless links. Wireless sensor networks are application, specific dynamic, and data centric and scalable. Sensor Nodes in network are made up of four components: processing unit, sensing unit, transceiver unit and power unit. Real time applications of wireless sensor networks are environment monitoring, health care, accident report, military field surveillance, and home application and flood detection. Lifetime and communication range of wireless sensor networks are short compared to Adhoc networks. Traditional nodes sense data individually and send it to base station in network and increases energy consumption.

Data aggregation technique is used to overcome all these limitations. Data aggregation is process of gathering data from sensor nodes and decides which data should be send to base station and when to send it. This technique reduces the number of transmissions and size of packets transmission in order to save the sensor energy and reduce transmission of redundant data. This technique helps in eliminating redundant data and saves energy.

Fundamental idea of data aggregation is to gather data from different sources in cluster, which helps in reducing number of transmission and also saves energy. There are many different data aggregation techniques based on network topology but it's very important to provide security to network while performing data aggregation, quality of services and network basis so that original data from sensor nodes can be received within short span of time.

2. Table

Comparison between WSN with and without Data Aggregation

	WSN With Data Aggregation	**WSN without Data Aggregation**
1	Eliminates redundant data and saves energy.	Cannot eliminate redundancy and consumes more energy.
2	Reduces the size and number of transmission.	Increase size and number of transmission.
3	With this process sensor nodes has ability to aggregate multiple packets into single packets.	Aggregation is not performed.
4	Node may consume more power whenever aggregated results sent to sink through uncompromised node.	Same data will be collected from different nodes.

5	Not applicable in all sensing environment.	Can be applied in all sensing environment.

3. Literature survey

Jinfang Jiang[1] et al, in this paper author has proposed EDTM trust model which provides trustworthiness in wireless sensor networks. The proposed model is compared with previous model NBBTE, where the results shows EDTM provides better performance compared to NBBTE. This model is used to keep neighbourhood information which provides significant less memory, less processing for trust calculations and low energy consumption.

Nanthini.D and R.A. Roseline[2], in this paper author concentrates on various types of data aggregation approaches in WSNs and the author describes each and every approach and protocol used for it. A better protocol is proposed after evaluating the performance all of protocols, which facilitates data aggregation and provides trustworthiness in network.

Sumeha Sirsikar and Samarth Anavatti[3], in this paper the author concentrates on issue and limitations in WSNs such as elimination of redundant data, reliability and delay. Different data aggregation approaches has different issues such as accuracy, traffic load, delay and redundancy in network. In this paper author selects some approaches to solve these issues and limitations. In wireless sensor networks data aggregation is performed at two levels, one at cluster head where cluster head acts as aggregator and other one at storage head. Thus data aggregation is performed at two levels in network and it maintains trade-off between accuracy, energy efficiency and maintains balance traffic load.

Ronald Watro, et.al [4], in this paper author describes TinyPk using public key technology. The communication security problems in wireless sensor network are exhausted because of limited battery power and energy of sensor nodes. Author uses symmetric key encryption to communicate safely. In this paper public key based protocol was designed and implemented. This protocol allows authentication and key agreement between sensor nodes and third party.

Xueying Zhang et.al [5], in this paper author design an energy efficient symmetric key cryptographic algorithm in wireless sensor networks. It calculates computational energy cost of cipher text by comparing number of CPU required to perform encryption and evaluates the performance of block cipher and stream cipher to noisy channel in wireless sensor networks.

Hu & Evans [6], in this paper author proposed secure data aggregation in wireless sensor networks. Author studied on data aggregation problem, when a node compromise. A lightweight mechanism is proposed to detect misbehavior node by this protocol. The proposed method main idea is on delayed aggregation and delayed authentication. In wireless sensor networks senor reading are forwarded to first hop without altering and data aggregation is done at second hop. Data aggregation is not done on immediate hop. Increases confidentiality and integrity but when parent and child hierarchy are compromised original data can be altered. The proposed scheme starts from leaf node by sending data, id, MCA to their parent node. Parent node stores all these and re-transmits to its parent node. Then parent node aggregate the data received from children's and grandchildren's and it re-transmit it to its parent. This process continuous until base station receives the data. Thus secure data aggregation protocol provides data freshness and integrity compared to traditional method.

4. Secure data aggregation

Data aggregation technique enables minimizing size and number of transmission in sensor network only when data aggregation carried out safely. Providing security to data aggregation process helps in receiving original information from sensor nodes. In wireless sensor networks appropriate measures need to be taken such as confidentiality of data, data integrity and authentication among communication nodes. Providing security to data aggregation should consider resources such as time, storage, computational and communicational efficiency requirements.

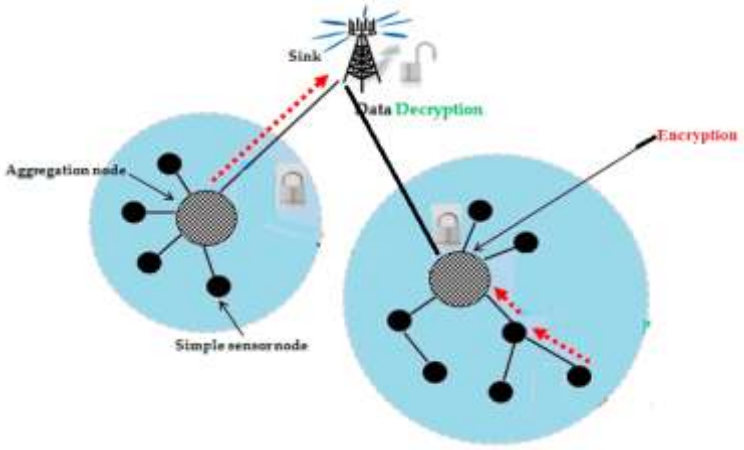

Fig 1: Wireless sensor network

In above figure1 encryption happens only on aggregated data at cluster head and transmits the cipher text to base station. Base station decrypts the received cipher text. Aggregation performed at cluster head and encryption doesn't takes place senor nodes and decryption is performed at base station using its own private key. In WSNs security is the major challenge in traditional security techniques and its algorithm. In many applications such as military, health and various application information is the critical component which need to be secured in efficient manner. Confidentiality of data: It makes sure that unauthorized user couldn't access to any private or sensitive in formation. Integrity of data: It assures that data in network are not changed and only authorized user can change the data. Freshness of data: To prevent the replay of old message at aggregate node data freshness is necessary. Confidentiality of data, data integrity and data authentication all these factors need to be taken care while selecting suitable approach to overcome limitations of traditional security techniques. Two types of secure data aggregation schemes are Hop-by-Hop and End-To-End.

A. Hop-By-Hop

Hop-by-Hop data aggregation sensor node sense the data and encrypts the sensed data and sends it to cluster head. Cluster head acts as aggregator node decrypts the received data and encrypts the aggregated data and then sends it to base station.

B. End-To-End

When end to end is compared with hop by hop, end to end has a flexible structure and routing protocol. In end to end data aggregation, sensor nodes encrypt the data and send it to cluster head, where cluster head directly aggregate the data without decrypting. So the sensor data provide end to end confidentiality and privacy.

Obstacles of sensor in network, compared to traditional networks are special networks with limited resources. It's difficult to apply existing security techniques in wireless sensor networks. In WSNs all the securities requires certain amount of resources for implementation which includes memory, code space and power. Issues such as unreliable communications among sensor nodes in network and it another threat to sensor nodes. Conflicts and latency. Sensors deployed in network, which are highly exposed to physical attacks.

5. Problem statement

Data aggregation enables the sensor networks in minimizing the size, number of transmission and energy consumption only when data aggregation process is carried out safely among sensor nodes in wireless sensor networks. A simple method can degrade the performance and complicates the security levels. Hence it is a challenge to find out a suitable cryptographic algorithm which over comes limitations such as network lifetime, redundant data and security to sensitive data communicated among the sensor node in a wireless sensor networks. Whereas asymmetric key encryption uses public key of base station to encrypt and base station decrypts cipher text using its own private key. Overall system security is high compared to symmetric key encryption and less affected by node compromising attacks. RSA algorithm is preferred in our project because the attacker cannot decipher or alter the data without knowing private key of base station even if public key is known.

6. Proposed method

Asymmetric key cryptography is also called as public key. It makes use of two different key for encryption and decryption purpose. Key distribution problem can eliminate using asymmetric key cryptography. Private Key must be secret. It is very difficult to decipher a message without private key. Asymmetric key cryptography are less affected by node compromising attacks compared to symmetric key. Public key cryptography achieves confidentiality, integrity authentication. In RSA algorithm, only public key of destination is shared and private key of it is not shared.
Following are the stages of process in wireless sensor networks.

A. Iterative Filtering Algorithm

Sensor nodes initialize the network parameters and configure all the parameters to all the nodes and deploy the nodes to NAM window. Finally deployed with nodes in network. The sensor nodes broadcast hello message to all the nodes and find the neighbour node with the help of hello message and repeat the same process for all the nodes and stores the information. Sensor nodes elect cluster head from sensor node having high RSS and energy and cluster head acts as aggregator node to perform aggregation. Sensor nodes calculate Bias estimation, Variance estimation and MLE. Errors in sensors nodes can be modeled by Gaussian distribution random variable and estimates bias value. The bias value defines matrices, computes matrices and estimates variance of sensor nodes. Estimated bias is subtracted from sensors reading and un biasing sensors reading and using MLE method to estimate the reputation vector without any vector. Reputation vectors are used to estimate the trustworthiness of each sensor. Based on distance of sensor reading reduces the number of iteration. Finally data is aggregated at cluster head.

B. RSA Algorithm

RSA is the public key cryptography and it is widely used for sensing data and transmitting in WSNs. RSA algorithm consist of three phases, they are prime key generation, encryption and decryption phase.

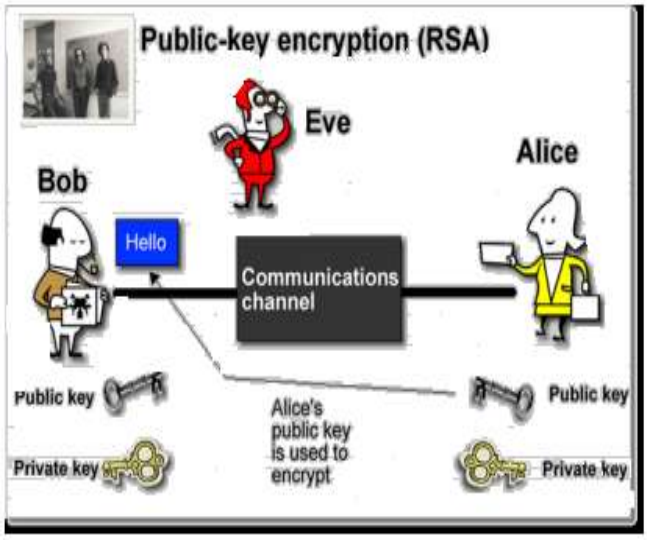

Figure 2: RSA Algorithm

In Above figure 2, Alice private key consists of {d, n} and its public key of consists of {e, n}. When source Bob wishes to send a message M to Alice, Bob encrypts message M using public key of destination. Public key is available only when Alice publishes it to Bob. Then Bob calculates $C = m^e \pmod n$ and transmits C to Alice. The user Alice decrypts cipher text using its own private key by calculating $M = c^d \pmod n$. RSA algorithm is performed on aggregated data at cluster head, which encrypts the aggregated data using public key of destination and decrypts using destination private key.

7. Implementation

Using NS2 simulation tool sensor nodes are created and deployed in an environment. Then forms cluster where each cluster has cluster head which acts as aggregator node. A sensor node send data to cluster to check any error in data and then estimates value such as bias, variance, and MLE. Once aggregated data is sent to base station then the input taken from receiver is encrypted at cluster using public key of base station and sent to base station which decrypt the received data using its private key.

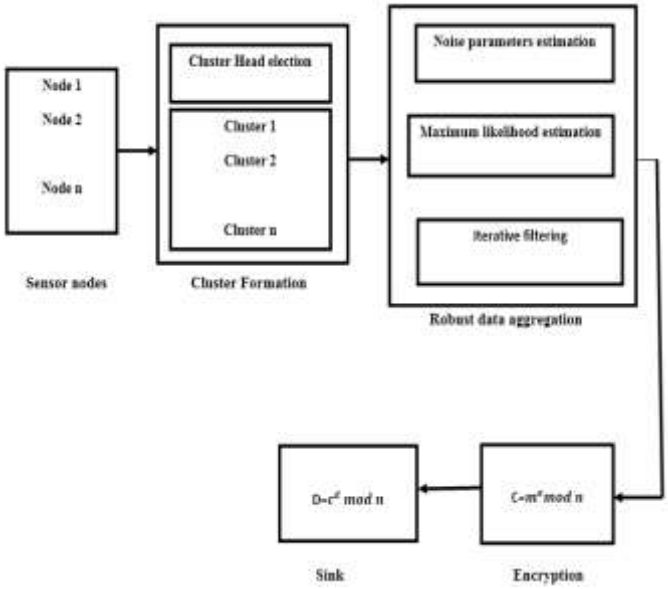

Figure 3: System Architecture

A. Node Creation

It is a process of creating sensor nodes in a wireless network. Once nodes are created in wireless network then each node sense information and communicate with other node in network.

B. Neighbour Discovery

In WSNs each node finds their neighbour nodes. Each node send hello message to each other node in cluster. It also reveals all possible paths between nodes in network. Through distance between nodes in wireless network neighbour discovery is achieved.

C. Data Aggregation

Using simulator bias, variance and MLE values are evaluated using iterative filtering algorithm which establishes trustworthiness and reduces redundancy and data traffic. Using this single iterative procedure compromised nodes are blocked from communicating to cluster.

D. Encryption technique

The aggregated data is communicated with base station in a secured manner using RSA algorithm. The phases are Key generation, encryption, and decryption.

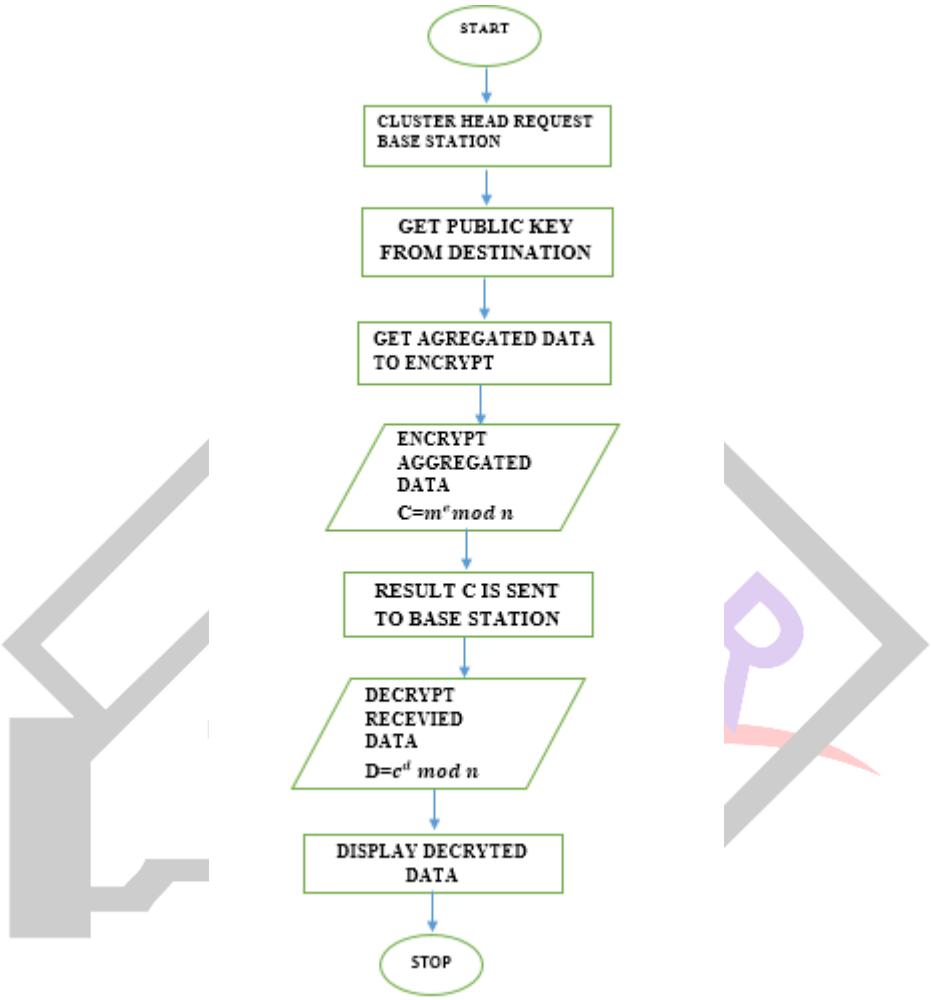

Figure 4: Public key encryption in WSN

Above Figure 4 shows public key encryption process in wireless sensor networks. In encryption process base station distributes its public key to all the cluster heads in a network. To find the public key of base station cluster head choose two large prime numbers p and q randomly and then calculates the value of n where n=p*q. Then calculates the quotient value using formula f(n)=(p-1)*(q-1). Then cluster head randomly selects a prime number e which is relatively prime to f(n) and e should be greater than 1 and less than f(n). f(n) should not be divisible by e. Finally cluster head know the public key {e,n}, then cluster head encrypts the data using formula: **C=M^e mod n** . Then encrypted data "C" is sent to base station.

Base station calculates the value of d using formula **d=e-1 mod f(n)** and then private becomes {d, n}. Then base station decrypt the received data using formula **D=$C^d$$mod$ n**. After completion of simulation the results in NS2 will be text based. Animation tool and Xgraph are used to represent the text based results graphically and interactively. Through this tools particular behaviour of nodes in network can be analysed, extracts the text based results and transforms into more conceivable presentation.

8. Conclusion

In design of any communication protocol energy consumption is the main objective in wireless sensor networks. Most of energy is consumed in transmission of bits among sensor nodes in network. Therefore energy consumption should be reduced

through data aggregation using iterative filtering algorithm which helps in eliminating redundant data.Second important objective of any communication protocol of WSNs is security. While data aggregation eliminates redundant data but it complicates data integrity. Hence in order to ensure security levels RSA algorithm is performed on aggregated data at cluster head, which guarantees end-to-end confidentiality.

References

[1] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Member, "*An Efficient Distributed Trust Model for Wireless Sensor Networks*" IEEE, and Mohsen Gu izani, Fello w, *IEEE Transactions On Parallel And Distributed Systems*, Vo l. 26, No. 5, May 2015.

[2] Nanthini.D and R.A.Roseline, "*Aggregation Protocols in Wireless Sensor Network- A Survey*" by International Journal of Advanced Research in Computer Engineering & Technology (*IJA RCET*) Volume 3 Issue 7, July 2014.

[3] Sumedha Sirsikar, Samarath Anavatti. "*Issues of Data Aggregatiom Methods in Wireless Sensor Network: A Survey*" in Proceedings of 4th International Conference on Advances in Computing, Communication and Control (*ICAC3'15*) Science direct 2015.

[4] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner. "*TinyPK: Securing Sensor Networks with Public Key Technology*" Copyright 2004 *ACM* 1-58113-972-1/04/0010.

[5] Xueying Zhang, Heys, H.M.; Cheng Li ." *Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks*", Communications (*QBSC*), 2010 25th Biennial Symposium.

[6] L. Hu, D. Evans."*Secure Aggregation for Wireless Networks*", in Symposium on Applications and the Internet Workshops, 27-31 January 2003, pp. 384-391.

[7] Luk, M, Mezzour, G. ; Perrig, A. ; Gligor, V. "*MiniSec: A Secure Sensor Network Communication Architecture* ", Information Processing in Sensor Networks, 2007. IPSN 2007. 6th *International Symposium*.

[8] Yang Zhao a, et.al ,"*A co-commitment based secure data collection scheme for tiered wireless sensor networks*" in 2010, Published by *Elsevier* B.V.doi:10.1016/j.sysarc.2010.05.010.

[9] N. S. Patil, P. R. Patil. "*Data Aggregation in Wireless Sensor Network*", in *IEEE International Conference on Computational Intelligence and Computing Research*, 2010.

[10] L. Zhu, Z. Yang, J. Xue, and C. Guo. "*An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks*", in *International Journal of Distributed Sensor Networks*, Hindawi Publications, 2014.

[11] R. Lathamanju,P. Senthilkumar. "*CRSR Algorithm: A Secure Data Aggregation Algorithm in WSN*", in *International Journal of Advanced Research in Electronics and Communication Engineering*, Volume 2, Issue 9, September 2013.

[12] Shih-I Huang, Shiuhpyng Shieh, J. D. Tygar." *Secure encrypted-data aggregation for wireless sensor networks*", *Springer Science* 2009.

[13] Kaushal J. Patel, Nirav M. Raja." *An Overview of Secure Data Aggregation in Wireless Sensor Network*" *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 5, Issue 1, January 2015.(ISSN 2277 128X).

[14] Sumedha Kaushik. "*Network Security Using Cryptographic Techniques*", *International Journal of Advanced Research in Computer Science and Software Engineering*, 2012.

[15] Saurabh Singh. "*Security for Wireless Sensor Network*", *International Journal on Computer Science and Engineering*, 2011.

[16] Mini Malhotra."*Study of Various Cryptographic Algorithms*", *International Journal of Scientific Engineering and Research*, 2013.

[17] Sirwan A. Mohammed. "*Design And Simulation Of Network Using Ns2", International Journal of Electronics, Communication & Instrumentation Engineering Research and Development*, 2013.

[18] Narender Tyagi. "*Comparative Analysis of Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering*, 2014.

[19] Dona Maria Mani. "*A Comparison between RSA and ECC In Wireless Sensor Networks", International Journal of Engineering Research & Technology (IJERT),* 2013.

[20] Annapoorna Shetty. "*A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm", International Journal of Innovative Research in Computer and Communication Engineering*. October 2014.

[21] Ankush Sharma. "*Implementation & Analysis of RSA and ElGamal Algorithm", Proceedings of the National Conference on 'Advances in Basic & Applied Sciences*, (ABAS-2014).

[22] S.Roy, M.Conti, S.Setia, and S.Jajodia. "*Secure Data Aggregation in Wireless Sensor Networks", in IEEE International Conference*, 2012.

[23] P. D. Patel, P.B. Lapsiwala, R.V. Kshirsagar, "*Data Aggregation in Wireless Sensor Network", International Journal of Management*, IT and Engineering, vol. 2, Issue 7 July-2012.

[24] S.Roy, M.Conti, S.Setia, and S.Jajodia, "*Secure Data Aggregation in Wireless Sensor Networks", in IEEE International Conference*, 2012.

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

[26] Aashima Singla, Ratika Sachdeva. "*Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, Issue 4, 2013.

[27] Vaibhav Pandey, AmarjeetKaur and Narottam Chand. "*A Review on Data Aggregation Techniques in Wireless Sensor Network", Journal of Electronic and Electrical Engineering* Vol.1, Issue 2, 2010

[28] Priyanka K. Shah and Kajal V. Shukla. "*Secure Data aggregation Issues in Wireless Sensor Network: A Survey", journal of information and communication technologies*, volume 2, issue 1, january 2012.

[29] Hani Alzaid Ernest Foo Juan Gonzalez Nieto. " *Secure Data Aggregation in Wireless Sensor Network: a survey", Conferences in Research and Practice in Information Technology (CRPIT),* Vol. 81, January 2008.

[30] Mr.Rakesh, Kr.RanjanMrs., S.P.Karmore . " *Survey on Secured Data Aggregation in Wireless Sensor Network" IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems* 2015.

[31] V.Vineel Ku mar, K.Ananda Brah mi. *" Data Aggregation Using Synopsis Diffusion Approach In Wireless Sensor Networks" International Journal of Innovative Engineering Research* (E- ISSN: 2349-882X) Vol 2, Issue 1, September 2014 .

[32] Mousam Dagar and Shilpa Mahajan. *"Data Aggregation in Wireless Sensor Network: A Survey", International Journal o f Information and Computation Technology*, Volume 3, Number 3, 2013. ISSN 0974-2239.

[33] un-won Ho. *"Distributed Detection of Node Capture Attacks in Wireless Sensor Networks"*, In Tech, Dec 2010.

[34] 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.