ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Secured Data Transmission in Wireless Sensor Network

P.Padmaja[1], Dr.G.V.Marutheswar[2]

Research scholar, Dept. of ECE, VITS, Nalgonda, Telangana, India[1]

Professor, Dept. of EEE, S.V.U. College of Engineering, Tirupati, Andhra Pradesh, India[2]

ABSTRACT: Data aggregation in Wireless Sensor Network (WSN) is applied to reduce redundancy and energy consumption. In WSN, in-network data aggregation performs aggregation of data in every router while forwarding data. Employing energy inefficient nodes in data aggregation affects lifetime of sensor network. Hence aggregation process in WSN should be optimized in energy efficient manner. When sensors are located in hostile environment, it is vulnerable to compromising attacks by adversaries. Compromised sensors inject false data during data aggregation process which results in false decision making at the Base Station (BS). Simple average data aggregation process is suitable only in attacker free environment. It is necessary to introduce a data aggregation mechanism that filters out attackers contribution during data aggregation. Behavior of nodes need to be observed in every round of data aggregation, and it should be reflected in subsequent rounds to filter out the impact of attacker contribution at the final result.If the aggregator is compromised, then it affects entire aggregation accuracy. Hence it is necessary to propose a aggregation protocol that is resilient against compromised sensor and compromised aggregator in energy efficient and secure manner.

KEYWORDS: Wireless Sensor Network, Cluster Head, Base Station, Secured Data Aaggrigation using Filter, Aggregation.

I.INTRODUCTION

wireless sensor networks (WSNs) consist of sensor nodes. These networks have huge application in habitat monitoring, disaster management, security and military, etc. Wireless sensor nodes are very small in size and have limited processing capability very low battery power. This restriction of low battery power makes the sensor network prone to failure. Data aggregation is very crucial technique in wireless sensor networks. With the help of data aggregation we reduce the energy consumption by eliminating redundancy. In this chapter discuss about data aggregation and its various energy-efficient technique used for data aggregation in WSN.

II.NEED FOR SECURITY IN WIRELESS COMMUNICTION

Wireless network is a network of wireless nodes that communicates with each other through radio waves or infrared waves. In wireless mode of message transmission the medium used for communication is invisible to the users. The nodes involved in wireless communication own short transmission range and mostly they are mobile nodes. Nodes within each others transmission ranges are allowed to communicate with one another. The main security issue caused in wireless network compared to wired network is the ease of accessing the transmission medium. The transmission medium is open to everyone and anyone can monitor or participate in communications performed in a wireless network. An adversary is able to listen to the information on transit or interfere with wireless communication.
Further, the short transmission range owned by sensor nodes led to hidden station problem which results in the collusion within the communications performed and may affect in loss of data. Any communications neglecting the basic security features such as confidentiality, authentication and integrity may pave the way for the unauthorised users to retrieve and disrupt the communications in transit.

Furthermore, the coordination packet is assumed to be small enough to be transmitted within slot duration. Instead of a common control channel, FHS provides a diversity to be able to find a vacant channel that can be used to transmit and receive the coordination packet. If a hop of FHS, i.e., a channel, is used by the primary system, the other hops of FHS

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

can be tried to be used to coordinate. This can allow the nodes to use K channels to coordinate with each other rather than a single control channel. Whenever any two nodes are within their communication radius, they are assumed to meet with each other and they are called as contacted. In order to announce its existence, each node periodically broadcasts a beacon message to its contacts using FHS. Whenever a hop of FHS, i.e., a channel, is vacant, each node is assumed to receive the beacon messages from their contacts that are transiently in its communication radius.

III.DIFFERENT ATTACKS IN WSN

In this There are different types of attacks in wireless sensor networks,they are

A. Selective Forwarding Attack (SF)

It is sometimes assumed that each node will accurately forward receive messages. However, a compromised node may refuse to do so. It is up to the adversary that is controlling the compromised node whether to forward received messages or not (Chris and David 2003). To put it in another way, the process of stopping the propagation of certain messages at the compromised node is under the control of the adversary. Once the adversary has succeeded in launching a SF attack, it can affect the propagation of the reputation information, such as direct observations across the network. Note that SF attacks are most effective when the attacking nodes are included in the path of the data flow.

B. Replay Attack (RE)

Some WSN applications are vulnerable to replay attacks where an adversary is able to eavesdrop on the traffic and replay old messages. Replay attacks are the easiest, because the adversary does not need to physically capture a sensor node and get access to its internal memory, or analyze intercepted encrypted data. In the reputation-based applications context, an adversary can record some reputation information, which has been exchanged wirelessly between sensor nodes, without even understanding its content and then replay them (with no changes) to mislead other nodes and make their reputation tables out-dated.

C. Spoofed Data Attack (SD)

In this type of attack, an adversary alters intercepted data in order to inject false data into the network and affects the reputation values. This attack cannot be launched alone; the adversary needs to combine either a RE attack or node compromise attack with a SD attack. In the former, the adversary first eavesdrops on the traffic, captures some reputation information in understandable format, performs some changes on the captured information, and then reinjects it into the network.

D. Node Capture Attacks

The process of getting hold of the sensor node through a physical attack is termed as node capture attack. There are two types of node capture attacks possible,they are Random node capture attack and Selective node capture attack.Random Node Capture Attack is in wireless sensor network, an assumption is made that each node will accurately send the message to their linked nodes in a normal scenario. When the attack is made on the node randomly, the node becomes adversary sensor. As a result the communication will be get break with their linked nodes; this causes the damage in the part of the network. So the random-node capturing is weak. Selective Node Capture Attack is this attack is mainly focused on the centralized node in order to expose its attack to more number of nodes. The central node in the network is selected; the attack is made which leads to the node to be an adversary node. Once the central node is attacked, this will disconnect all their linked nodes which lose its communication. As a result the whole network will get collapsed. So the selective node capture attack is very harmful, particularly when the nodes are in the form of data flow.

IV. PROPOSED SYSTEM

An optimized and secure data aggregation protocol is proposed that is resilient to false data injection attack launched by compromised sensor and aggregator. Proposed protocol with the support of energy efficient clustering, performs secure data aggregation process along with trustworthiness estimation using Trust wEighted Secure Data Aggregation algorithm (TESDA). Data aggregation process is optimized by performing aggregation in energy efficient manner through clustering. Sensor network is divided into clusters and each energy efficient Clusterhead (CH) aggregates data collected from its cluster members and transmits to BS. Secure data aggregation is carried out in two phases first at the aggregator to make it resilient against compromised sensors and second at BS to make it resilient against compromised aggregator.

In first part of research work CH aggregates weighted average of reported value by each sensor in its cluster. Weight parameter is applied to reduce the impact of contribution of compromised sensor in the aggregation result. Trust value

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

of the sensors is transformed into weight. Trust value of the sensor data is computed from the non deviation factor. Deviation is computed as the difference between aggregated value and the original value reported by the sensor. If the deviation is high then trust value is reduced. When the false data is injected by the compromised sensor, high deviation results in low trust value and weight that reduces the impact of attacker contribution in the final result.
In second part of research work, BS executes verification mechanism to check the validity of the aggregation result reported by the CH. it selects subset of nodes from each cluster and queries original data from those nodes. The data from those sensors are propagated without aggregation. BS aggregates the received information from the sensors. Then it computes the deviation of aggregated result from the reported value by CH. The trust value for the CH is estimated from the computed deviation. If the CH is compromised its deviation becomes high that results in reduced trust value. Hence the contribution of the compromised CH is reduced at the BS.Proposed protocol is optimized through cluster based data aggregation process and security is enhanced by making the protocol resilient against compromised aggregator along with compromised sensor.Trustworthiness measurement in proposed work, assist in secure data aggregation process as well as other network processes such as trust based routing, trust based cluster head selection.

V. SIMULATION MODEL

Simulation model for the proposed system is given in below table 1

TABLE I. Parameters Used For Simulation

SIMULATOR	Network Simulator 2
NUMBER OF NODES	30,40,50,60
AREA	500m x 500m
COMMUNICATION RANGE	250m
INTERFACE TYPE	Phy/WirelessPhy
MAC TYPE	802.11
QUEUE TYPE	Droptail/Priority Queue
QUEUE LENGTH	200 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	TwoRayGround
ROUTING AGENT	TESDA
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
INITIAL ENERGY	50 Joules
TRANSMISSION POWER	0.3watts
RECEPTION POWER	0.1watts
SIMULATION TIME	30seconds

VI. MODULES

- Optimized Data Aggregation via Energy Efficient Clustering.
- False Data Injection Attack.
- Secure Data Aggregation - Resilience against Compromised Sensors.
- Secure Data Aggregation - Resilience against Compromised Aggregator.
- Performance Evaluation.

A. Modules Description

i. *Optimized Data Aggregation via Energy Efficient Clustering*

Input: Sensors ID and Residual energy

Output: Clusterhead

Each sensor attaches its ID and residual energy in its hello message. The node that receives the hello message add the sender in its neighbor list. Each node compares the residual energy of all of its neighbors. It selects the neighbor that has high residual energy as its ClusterHead (CH). Cluster member attaches its CH ID in hello message. On receiving hello message each node checks whether the CH ID mentioned in the hello message and its own ID are same. If it so it

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

adds the corresponding sender its its member list. CH roles are rotated in every round in order to balance the energy consumption. Clustering rounds depends on the clustering period.

ii. False Data Injection Attack

Input: False data through compromised sensor

Output: Falsified aggregate Sensed result (X) of every sensor (S_i) is submitted to CH. It derives the aggregated result (A_r) by taking weighted average of collected information. Attacker compromises the sensor and alters its sensed value to very low or high to distort the aggregation result. False data from compromised sensor, reduces aggregation result as CH computes aggregation result from the reported value. When the CH submits the falsified aggregate to the base station, it leads to false decision making.

$$\text{Aggregated result } A_r = \sum_{i=1}^{n} X_i /n \quad r=1,2..m$$

iii. Secure D

Input: False data through compromised sensor, actual data from genuine sensors.

Output: Reduced trust of compromised sensor, Filtered attacker contribution in aggregated result .Sensed result (X) of every sensor (S_i) is submitted to CH. It derives the aggregated result (A_r) by taking weighted average of collected information. Weight of the every sensor is assigned from the trust measurement of the sensor. Trust of every sensor is evaluated from Non Deviation Factor. If the non deviation factor is low trust becomes very low which means that its value is deviation is high. Attacker compromises the sensor and alters its sensed value to very low or high to distort the aggregation result. As the aggregator computes trust value from the deviation, compromised sensor gets very low trust. Hence contribution of the corresponding sensor is reduced in aggregated result as trust is considered as weight in computation. Final aggregated result at CH is the trust weighted summation of data reported by the cluster members of the cluster in the round.

$$\text{Average Data } (Avg_r) = \sum_{}^{n} X_i \quad r=1,2..m$$

$$\text{Deviation } D(r) = \quad \text{Avg}_r \sim X_i(r)$$

$$\text{Total Deviation } TD(r) = \sum_{i=1}^{n} D_i(r)$$

$$\text{Non Deviation Factor } NDF_i(r) = TD(r) \sim D_i(r)$$

$$\text{Total Non Deviation } TNDF_i(r) = \sum_{}^{n} X_i$$

$$\text{Trust } T_i(r) = NDF_i(r) / TNDF_i(r)$$

$$\text{Weight } w_i(r) = T_i(r)$$

$$\text{Aggregated result } A_r = \sum_{i=1}^{n} w_i X_i \quad r=1,2..m$$

iv. Secure Data Aggregation - Resilience against Compromised Aggregator

Input: False data through compromised aggregator, actual data from genuine aggregators.

Output: Reduced trust of compromised aggregator, Filtered attacker contribution in aggregated result. If the attacker compromises the CH, it alters the aggregated result (Z_i) before submitting it to the Base Station (BS) in order to distort the final aggregation result ($BS(A_r)$) at the base station. To overcome this issue BS verifies the trustworthiness of the CH (TCH_i) through the original sensed information collected from the subset of CH nodes (k) . BS aggregates the collected data from subset of CH nodes and finds the deviation (DCH_i) between reported result by CH. If the deviation

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

is high BS reduces the trust value of the CH as the inverse proportion of the deviation and direct proportion of the non deviation factor (NDF_CH). Hence the impact of falsified data contributed by the CH is reduced at the base station. Final aggregated result at BS is the trust weighted summation of data reported by the CHs in the round.

$$\text{BS Average Data } (BSAvg_r) = \sum_{i=1}^{k} Z_i \qquad r=1,2..m$$

$$\text{Deviation } DCH_i(r) = BSAvg \sim Z_i(r)$$

$$\text{Total Deviation } TDCH(r) = \sum_{k} DCH_i(r)$$

$$\text{Non Deviation Factor } NDF\_CH_i(r) = TDCH(r) \sim DCH_i(r)$$

$$\text{Total Non Deviation } TNDF\_CH_i(r) = \sum_{k} NDF\_CH_i(r)$$

$$\text{Trust } TCH_i(r) = NDF\_CH_i(r) / TNDF\_CH_i(r)$$

$$\text{Weight } w_{chi}(r) = TCH_i(r)$$

$$\text{Aggregated result } BSA_r = \sum_{i=1}^{k} w_{chi} Z_i \qquad r=1,2..m$$

The TESDA based proposed approach is evaluated and compared with existing approach Secure Data Aggregation in WSN using Filtering (SDAF) [1] for the following parameters using the ns-2 simulation.

- **Data Aggregation Deviation**
  It refers to the percentage of the aggregation error. It is calculated as the ratio of deviation to the true value sensed by the sensors.
- **Network lifetime**
  It refers to the time till half of the nodes in network remains alive. It refers to the total number of control packets involved for the secure data aggregation process.
- **Overhead Attacker Impact Reduction Ratio**
  It refers to the ratio of reduced trust of the compromised sensors from the actual trust of the compromised sensors resided in the network
- **Energy Consumption**
  It refers to the total amount of energy required for data aggregation process.

VIII. RESULTS AND DISCUSSION

A. Comparison of TESDA and SDAF

i. Data Aggregation Deviation

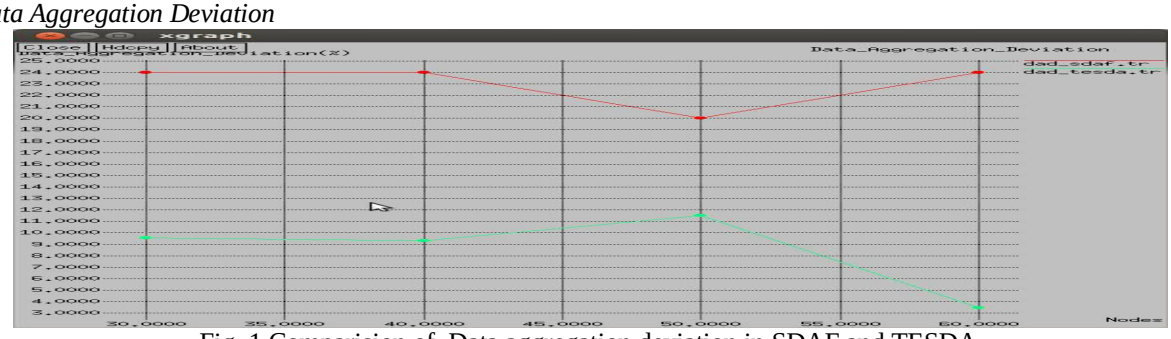

Fig. 1.Comparision of Data aggregation deviation in SDAF and TESDA

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Data aggregation deviation is reduced in proposed protocol TESDA than existing protocol SDAF. Because, proposed protocol finds the aggregated result based on the deviation of the values reported by all the sensors in the cluster. But SDAF simply takes OR operation of received synopsis without considering deviation. With the increasing number of sensors, number of genuine sensors are increased that reduces the aggregation deviation.

ii. Network lifetime

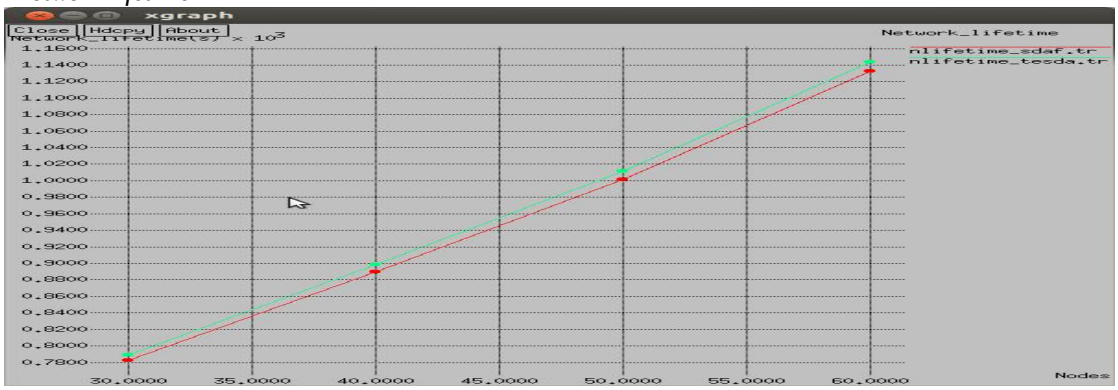

Fig. 2.Comparision of Network lifetime SDAF and TESDA

Network lifetime of TESDA is improved when compared to SDAF because, SDAF incurs control packets for verification of MAC. In the case of invalid MAC it broadcast control packets for to fins valid MAC for the received bit which is not the case in TESDA.

iii. Overhead:

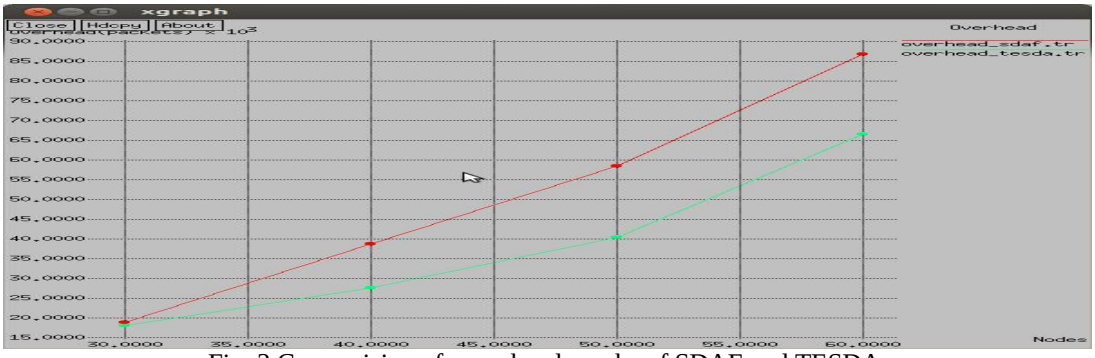

Fig. 3.Comparision of over head graphs of SDAF and TESDA

Overhead of SDAF is high when compared to TESDA because, SDAF incurs control packets for verification of MAC. In the case of invalid MAC it broadcast control packets for to fins valid MAC for the received bit which is not the case in TESDA.

iv. Attacker Impact Reduction Ratio

Attack impact is reduced in TESDA when compared to SDAF because it takes the aggregation based on deviation but where as in SDAF, deviation is not considered for aggregation.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

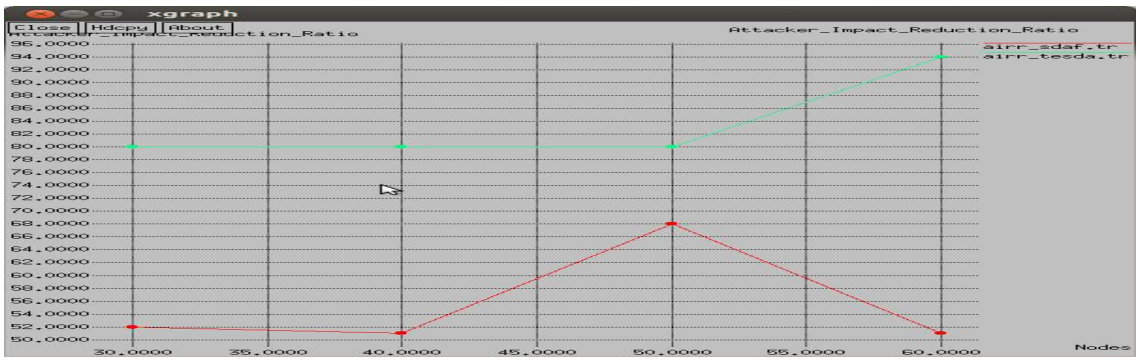

Fig. 4. A comparision graph of attckers impact reduction ratio of SDAF and TESDA

v. Energy consumption

Energy consumption is reduced in TESDA when compared to SDAF because of the reduced control packets involvement. It increases when the number of nodes are increased due to the increased overhead.

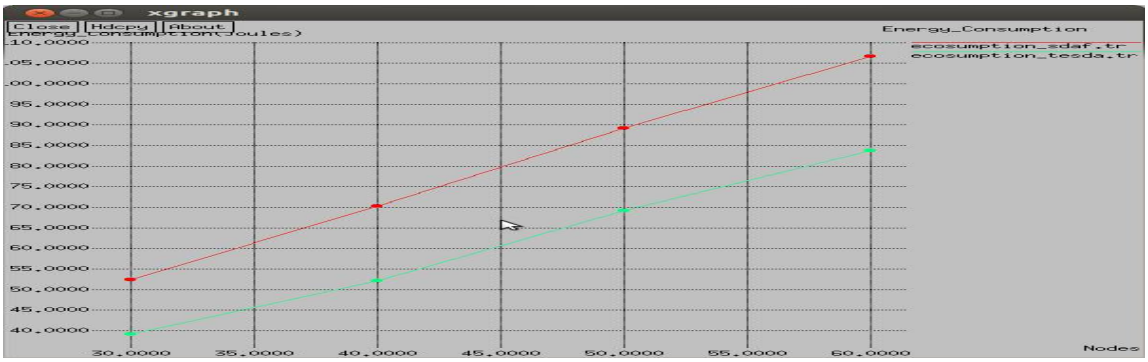

Fig. 5. A comparision graph Energy consumption in SDAF and TESDA

IX.CONCLUSION

From analysis of result TESDA is the best method for secured data aggregation at both cluster headl and base station .Future scope of development of this algoritham by increasing number of node and optimizing node energy **.**

REFERENCES

[1] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen and David E. Culler “SPINS: Security Protocols for Sensor Networks”, Journal of Wireless Networks, Vol. 8, No. 5, pp. 521-534, 2002.

[2] Ahmed, A. A., Shi, H. and Shang, Y. “A Survey on Network Protocols for Wireless Sensor Networks”, Proceedings of the International Conference on Information Technology Research and Education (ITRE), pp. 301-305, August 2003.

[3] Akkaya, K. and Younis, M. “A Survey on Routing Protocols for Wireless Sensor Networks”, Journal of Ad-hoc Network, Vol. 3, No. 3, pp. 325-349, May 2005.

[4] Al-Karaki, J. N. and Kamal, A. E. “Routing Techniques in Wireless Sensor Networks: A Survey”, IEEE Transaction on Wireless Communications, Vol. 11, No. 6, pp. 6-28, December 2004.

[5] Amrita Ghosal and Jyoti Prakash Singh “Secure Data Aggregation Using Some Degree of Persistent Authentication in Sensor Networks” Proceedings of the Conference on Mobile and Pervasive Computing (CoMPC-2008), pp. 183-186, August 2008.

[6] Aravind Iyer, Sunil S. Kulkarni, Vivek Mhatre and Catherine P.Rosenberg “A Taxonomy-Based Approach to Design of Large-Scale Sensor Networks”, proceedings of the Conference on Wireless Sensor Networks and Applications, Signals and Communication Technology,pp. 3-30, 2008.

[7] Banerjee, I., Chanak, P., Sikdar, B.K. and Rahaman, H. “EER: Energy Efficient Routing in Wireless Sensor Networks”, Proceedings of the IEEE Students' Technology Symposium (TechSym) pp. 92-97, Jan 2011.

[8] Algorithms”,Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR’04), Phoenix, pp. 241-245, April 2004.

[9] Roy, Sandip, et al., "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", IEEE Transactions on Information Forensics and Security, Vol.9, No.4, pp.681-694, 2014.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

[10] Zhu W, Xiang, Y & Zhou, J 2011, 'Secure localization with attack detection in wireless sensor networks', International Journal of Information Security, vol. 10, no. 3, pp. 155-171.
[11] Pradeepa,K,Anne,WR&Duraisamy,S 2012,'Design and implementation issues of clustering in Wireless Sensor Networks', International Journal of Computer Applications, vol. 47, no. 11. pp. 23-28.
[12] Kavitha, T & Sridharan, D 2010 'Security vulnerabilities in Wireless Sensor Networks: A survey', Journal of Information Assurance and Security, vol. 5, pp. 31-44.
[13] Daojing He, Jiajun Bu & Chan, S 2011, 'Privacy- preserving universal authentication protocol for wireless communications', IEEE transactions on wireless communications, vol. 10, no. 2, pp. 431-436.
[14] Alcaraz, C, Lopez, J & Roman, R 2012, 'Selecting Key Management Schemes for Wireless Sensor Networks application', Journal of Computers and Security (Elsevier), vol. 31, no. 8, pp. 956-966.
[15] Azarderskhsh, R & Reyhani, A 2011, 'Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks', Eurasip Journal on Wireless Communications and Networking, Article ID: 893592, pp. 1-12.
[16] Lopez, J, Roman, R & Alcaraz, C 2009, 'Analysis of security threats, requirements, technologies and standards in Wireless Sensor Networks', Journal of Foundations of security analysis and design, vol. 5703, pp. 289-338.
[17] Padmaja P,Marutheswar ,G.V ,2016,'Secured Data Aggregation In Wireless Sensor Networks',International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 7 (2016) pp 4740-4745.
[18] Padmaja P,Marutheswar ,G.V ,'Optimization Of Wireless Sensor Network' proceedings of the Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) pp. 161-165, Jan2016.
[19] Padmaja P,Marutheswar ,G. V ,'Optimization Of Wireless Sensor Networks In Secured Data Aggregation 'International Journalof Electrical and Electronis Engineering Research ISSN 2321-2055Volume 7, Number 2 (2016) pp 94-100.