International Journal of Engineering & Technology, 7 (1.1) (2018) 594-598

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Detecting malicious nodes using data aggregation protocols in wireless sensor networks

P. Balamurugan[1*], M. Shyamala Devi[2], V. Sharmila[3]

[1]*Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Chennai, India*
[2]*Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Chennai, India*
[3]*K.S.R. College of Engineering, Tiruchengode, India*
**Corresponding author E-mail: pookumbala@gmail.com*

Abstract

At present scenario, sensor devices are used in various fields for gathering information so all those data should be secured safely. Securing data is an important role in Wireless Sensor Networks (WSN). WSN is extremely essential for the purpose of reducing the complete redundancy and energy consumption during gathering data among sensor nodes. Optimized data aggregation is needed at cluster head and Base Station (BS) for secured data transmission. Data aggregation is performed in all routers while forwarding data from source to destination node. The complete life time of sensor networks is reducing because of using energy inefficient nodes for the purpose of aggregation. So this paper introduces the optimized methods for securing data (OMSD) which is trust based weights and also completely about the attacks and some methods for secured data transmission.

Keywords: *Securing Data, Aggregation, Sensor, Energy, Attack, Network Lifetime And Overhead.*

1. Introduction

In recent years, mobile communications and wireless networking technology have noticed a considerable expansion. With the assistance of technological advancements together with application demands, several classes of communication networks have emerged for instance, Ad hoc Networks, Sensor Networks Cellular networks and Mesh Networks. A sensor network characteristically includes a vast number of sensor nodes densely organized in a section of importance, and supplementary data sinks or BS that are located nearly or within the recognizing region, as revealed in Fig.1. It must be observed that the sink(s) handovers queries to the subsequent sensor nodes at the same time the sensor nodes team up to finish the sensing job and handover the detected data to the particular sink(s). In the meantime, the sink(s) furthermore serves as a gateway to external networks, for instance, [1] the Internet. It completely gathers data from the sensor nodes, accomplishes simple processing on the gathered data, and subsequently transmits associated details over the Internet to the users who demanded the data.

WSN are extremely vulnerable to security attacks because of the broadcast environment of the transmission medium. In addition, WSNs have an additional vulnerability since nodes are located in an aggressive or dangerous atmosphere where they are not physically protected. Fundamentally attacks are categorized as active and passive attacks [2].

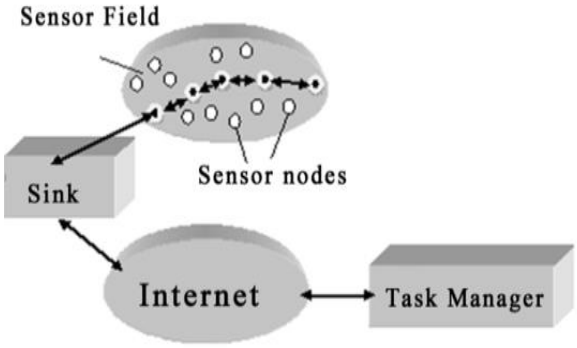

Figure 1: Wireless sensor network

Passive attacks

Here, the observation and listening of the communication channel through unauthorized attackers are known as passive attack. All the attacks in contradiction of privacy are passive in nature.

Attacks against Privacy: The major privacy complication is not that sensor networks allow the gathering of information. Relatively, WSN deepen the privacy complication since they make huge volumes of information straightforwardly available through remote access. Therefore, adversaries need not tangibly exist to preserve scrutiny. It could collect information at small-risk in undisclosed mode. The mutual outbreaks [3] in contradiction of sensor privacy are listed below:

Monitor and Eavesdropping: In case if the traffic sends the control details regarding the WSN configuration, which comprises possibly more comprehensive data than certainly extended over the location server, the eavesdropping can carry out skilfully in contradiction of the privacy protection.

Traffic Analysis: Despite the fact if the transmitted messages are completely encrypted, it still offers a great chance of examination of the message configurations.

Camouflage Adversaries: It is possible that one can attach their node or absolutely negotiate the nodes for the purpose of hiding. Following that, these kinds of nodes can effectively copy as a standard node for the purpose of drawing the packets through their path, then misroute the packets, executing the privacy analysis.

Active attacks

The illicit attackers observes, pays attention to and transforms the data stream in the communication medium are recognized as active attack. Few active attacks are Denial of Service Attacks, Routing Attacks in Sensor Networks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, False Node, Message Exploitation, Passive Information Gathering, Node Replication Attacks, etc.

Security goals for WSNs

In case of application layer the category of attack is normally subversion and malicious nodes. The major action against these attacks is that malicious node detection and isolation. At the point of network layer the type of attack is normally Sinkholes, Wormholes, Sybil. The major action against these attacks is Key Management, Secure Routing, In case of Data Link Layer, the attack category is Layer Encryption. The major action against these attacks is that is capture. In case of Physical Layer the category of attack is DoS and Node. The major action against these attacks is that is adaptive antennas, Spread Spectrum.

Physical Attacks: The attacker achieves straight admission to the hardware. It enables a DoS kind of attack: they can simply eradicate the nodes. It must be noted that the physical access also permits them the right of entry to a node's elements devoid of any software layer comprised. It is in contradiction of a remote attack, in which the attacked system is processed with the assistance of certain protocol or application layer, that provides the possibility for sensing the kind of attack and respond consequently. In case of a physical attack, this category of "self-surveillance" is not accessible to the hardware further down the attack and be conceivable through supplementary measures, for instance peripheral investigation. Hence, physical attacks very dominant.

Its major advantages comparing to remote attacks are as given below:

- The attacker has some information regarding the hardware that they are really going to attack. The the intermediate for all the remote attacks is network traffic, and effectively be point in the wrong direction easily, and verifying the uniqueness of a remote entity is extremely complicated. Physical attacks occur with direct access to the computer, which typically provides adequate details for consistently recognizing the hardware and its vendor. At some point when the attacker has turned out to be so adjacent, it possible impossible to distract his efforts to a less sensitive target.
- In the case if it is closer to a system, the maximum comes to be the available bandwidth. Remote attacks are extremely limited through network interfaces. It must be observed that the long-distance connection normally ranges from 64 kbit/s to 2Mbit/s. it must be observed that the wireless connection ranges from 128 kbit/s to 54 Mbit/s. Possibly, an attack happening inside a LAN ranges up to 1 Gbit/s. Moreover, straight wired interfaces permit comparable data speeds, such as, Fire wire.
- Sensitive information, are not likely to be reachable or else, could be obtained with the assistance of distinct device that is secretly connected with a system, e.g. a key logger for the purpose of recording user credentials.

Interface attacks: These kinds of attacks exploit vulnerabilities of the interfaces a device offers with the intention of allowing right of entry to its individual provisions or right of entry peripheral provisions. In case of wireless communication interfaces, possibly there could be noticeable attacks for instance, eavesdropping, traffic analysis, and message injection jamming. These processes are completely assisted through the wireless broadcast nature. At this point, valid commands are implemented in unfamiliar sequence, by this means provoking unintended behavior in favour of the attacker. It must be noted that, the service interfaces of sensor networks have not been examined based on the security vulnerabilities. Rather, lot of work has been carried out for the purpose of securing the wireless interface. It must be observed that the attacks on these interface of nodes are simple for executing, for the reason that they need simply a wireless transceiver. Moreover a peripheral device could be utilized, or captured nodes of the sensor network themself, following a positive physical attack on few nodes. There are certain transformation is in the exposure of the organization zone: an extraordinary-powered peripheral device possibly will empower the attacker to influence the entire nodes simultaneously, despite the fact that single sensor nodes possess a supplementary restricted radio limit. Few attacks scheduled in the place of transport layer possibly be let down without difficulty. Further attacks are not quite impossible to thwart, for instance, jamming. Few mitigation schemes are applicable, though. In case when only a restricted section is disturbed, it might be conceivable to route all over the place. In case of hybrid networks, that service supplementary wired connections, a overcrowded node possibly will give a signal or alert exterior to the overcrowded region. A chance for stopping overcrowding possibly be the exploitation of fixed optical rather than radio links, however those are extremely complicated to install.

Software level attack: These are the influential attack is the installation of code into an implementation background, in the meantime this provides possibly complete regulation on it. These kinds of attacks are common, most of the place are not well supervised hosts, which are effectively disposed to to adversarial remote control. One of the major intentions for this code mobility is tat the code is frequently transferred from distant sites and executed in the neighbourhood. Although tools are existing for code authorization, these are normally evaded through either social engineering or carelessness of the user.

Codes and tools for WSNs are habitually formulated by means of low-standard languages like C. hence, it enables the possibility of vulnerabilities like buffer overflows. Fortunately, microcontrollers are frequently dependent on the Harvard processor structural design, which substantially distinct program and data memory. In these kinds of structural design, buffer run-offs typically don't cause unsolicited program implementation, because maximum number of drivers don't inscribe into program memory openly. On the other hand, stirring to processors that are dependent on the von Neumann structural design, or by means of computer-generated machines exposes sensor networks to the risks of such vulnerabilities.

It must be noted that, custom software expansion can considerably lessen the danger of software-level attacks, subsequently the utilization of susceptibilities in these systems is

further expensive to an invader than compared to homogenous systems. Correspondingly, the lack of software lifecycle administration tools permits to construct these kind of restricted interfaces that additionally condense the risk of vulnerabilities. On the other hand, both schemes put severe constraints on the flexibility and the cost-effectiveness. Hence it is roughly observed that a considerably more exposed scheme will be typically employed in sensor networks in the upcoming years.
On the whole, it is simple distinguish concerning the primary and secondary goals that an attacker tracks. It must be observed that the primary goals look after the data stores the attacker wants to obtain full control on it. The attackers objective might be to obtain any undisclosed details, or disturb a service, or misrepresent certain data with the intention of hiding the occurrence of details, simply to reference few examples. The subordinate goals are taking care with the status quos of an attack.
It is accomplished that end-to-end schemes possibly be either expensive or pressuring in several applications of WSNs, hence considered the rough calculation of end-to-end security as an alternate scheme that delivers adequate security that is satisfactory for several purposes and possibly will put off potential attackers in several scenarios.

2. Proposed methods

Sensors collect the information from multiple sensors. Data collection will be single hop or multi hop communication. Then data are aggregated at an aggregator (sink node or head node) which forwards the aggregated values to the BS. OMSD which comprise of the three methods which are useful for detecting malicious nodes for securing data.

BASIC Scheme

Step 1: Identifies a new cosmopolitan collision attack against BASIC scheme dependent on reputation systems which discloses a heavy vulnerability of BASIC scheme.
Step 2: A scheme for the purpose of estimating the sensor errors which is operational in an extensive range of sensor errors and not vulnerable to the designated attack.
Step 3: Design of a well-organized and influential aggregation scheme which exploits an estimate of the noise parameters, acquired by means of contribution of above step1 and step2.
Step 4: Enhanced BASIC schemes capable of protection against sophisticated collision attacks by means of providing an initial estimate of trustworthiness of sensors by means of inputs from contributions of step 2 and step 3.
Step 5: BASIC scheme implemented on HEF and TEEN protocol to analyze the simulation performance.

EEFO algorithm

Energy efficient first order (EEFO) algorithm is another important secured data aggregation method. It is also used to change Cluster Head (CH) node in a region when it loses its energy.

Step1: CH formation

1. Initially all the nodes share with HELLO message to all neighboring nodes
2. All the nodes check their respective energy level with received energy level.
3. Finding the highest energy node among nodes being in one group. Then node with highest energy will act as CH node and intimate all other nodes in the group that is CH.

Step 2: message passing from source to BS.

if (route is existing in route table)
{
Check the energy consumption speed of CH
Precede the process for sending data to the destination
}
else {
Insert the new message in queue
}

Step 3:

if (consumption speed is high)
{
Precede the process for sending data to the destination
Forward the message
}
else{
Changing of the CH takes place based on the value
}

Mathematical model for energy consumption

The mathematical model which is used to find the energy level of each node for choosing the CH nodes which will coordinate the other nodes in each group. In the previous works, the first order radio model has been used to calculate the energy consumption for PEGASIS and LEACH in all simulations. According to this model[4], the transmitter electronics of each sensor node function at 50 nJ / bit sent. The same is true for receiver electronics with regard to bits received. 100pJ/bit/m^2 will be required to amplify the signal sent by the transmitter, and the radio will be shut down during down time to avoid unwanted reception of message. Thus, the total cost of transmission of **k** bits over a distance **d** will be governed by the equation.

$$E_{Tx}(k,d)=(E_{elec}\times k)+(\in_{amp}\times k\times d^2). \quad (1)$$

Whereas the cost of receiving and aggregating the data from **n** senders will be governed by the following equations:

$$E_{Rx}(k)=(E_{elec}\times k),n=1 \quad (2)$$

$$E_{Da}(k)=(5\times k\times n),n>1. \quad (3)$$

Where,
E_{Tx}-Energy for Transmitter,
E_{Rx}-Energy for Receiver,
E_{Da} -Energy for Data aggregation.
Each node is allotted an initial energy value of 1Joule in this model. A node has "failed" when its energy level falls below 0, due to energy loss from data transmission or reception. Based on the method or protocols the above equations (1), (2) and (3) are used to calculate the energy level of all nodes.

Safety level data aggregation (SLDA)

The nodes from different clusters send their data to aggregate nodes which are used to aggregate the data. The aggregator node is also a node that aggregates the data. Then it finds the distance of nodes and its trust values. In sensor networks the distance between two nodes are found out Using Euclidean Distance formula. Trusted nodes only send data to cluster head. The node's trust values are calculated based on the information in the packet. The aggregator compares each and every data. This task is performed by the variance estimator. If the data is more over the data comes for the malicious node. Maximum same data are comes from the goog node. This is not a single time process. It is the iterative process. It can identify the trust nodes by the data aggregation based on this approach. So this method can provide the SLDA.

Tree based model

Step 1: It finds the residual energy of each node in the network. Subsequently, elevated energy neighbor node is chosen as parent and it is ascribed through certain text data.
Step 2: After obtaining the text data, the subsequent node verifies its identification and the parent id indicated in the text data. Once it equals it includes the node to its member list.
Step 3: Every single node is attentive of child and its member list.
Step 4: Bitstring for every temperature data is computed for every sensor and transmitted to parent (CH).
Step 5: Every sensor generates MAC for it using its genuine key. After all data are received by parent, it access the synopsis and corresponding MAC.
Step 6: Operation of the received synopsis is computed by the parent. Then BS finds a sensor as attacker if its MAC is invalid and excludes corresponding data.
Step 7: BS verifies MAC for every received bit and if no valid MAC is found for a bit it discard the bit and broadcast control by querying valid MAC for the bit. Finally BS verifies received MAC and filters unauthorized bit from final fused synopsis.

3. Experimental setup

Simulation based experiments were conducted in this work to evaluate the performance of the proposed protocol. With the intention of analyzing the performance of the proposed scheme, the simulation was executed under the NS2. The simulator parameters are given in Table 1. The network area is restrained within 650×650 m^2. Every single node has a position and a velocity and travels about over a rectangular flat space. Every single node in the network has a transmission limit of 300m-300m. A two-ray ground reflection scheme is exploited as the radio propagation model. The MAC layer scheme uses the IEEE 802.15 MAC specification which is selected for the purpose of physical and data link layer, that is extremely appropriate in case of low data speed however extremely extended battery life applications.

Table 1: Simulation Parameters

Parameter	Value
Simulator	NS2 (NS-2.28)
Network Area	650 x 650 m^2
Transmission Range	50m-300m
MAC Layer	IEEE 802.15
No of Nodes	1000
Node Initial Energy per node	1 joule
Data Packet Size	164 bytes
Bandwidth	20 Mbps
Simulation Time	100 s
Processing power P_c	10^{-4}w
Receiving power P_r	$5*10^{-5}$w
Outage requirement e_{in}	10^{-4}
No of trial	10000
Confidence Interval	92%

Meanwhile, the transmission cost prediction comparatively based on previous works [5]. As a result, in case constraints necessary for the purpose of prediction progression, this paper continues to make use of identical values as implemented. Parameters are tabulated in table 1. Each single simulation includes a certain malevolent segment of the networks. All these defected nodes are traced arbitrarily in the simulation zone, and are allocated with definite behaviors that can additionally disturb the route detection progression.

4. Experimental results

The performance of the SLDA is compared with other data aggregation algorithms described previously through simulations to observe the advantages and disadvantages of the SLDA. The network lifetime, energy consumption, network overhead and attacker impact on network metrics are measured to analyze the performance of the proposed system. The fig.2 shows that network lifetime of SLDA is improved when compared to EEFO.

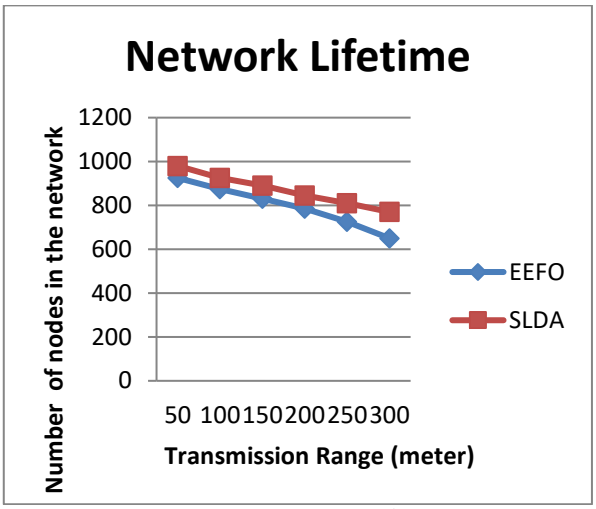

Figure 2: Transmission range vs. number of nodes in the network

The fig.3 shows that Energy consumption is reduced in SLDA when compared to EEFA because of the reduced control packet involvement. It increases when the numbers of nodes are increased due to the increased overhead.

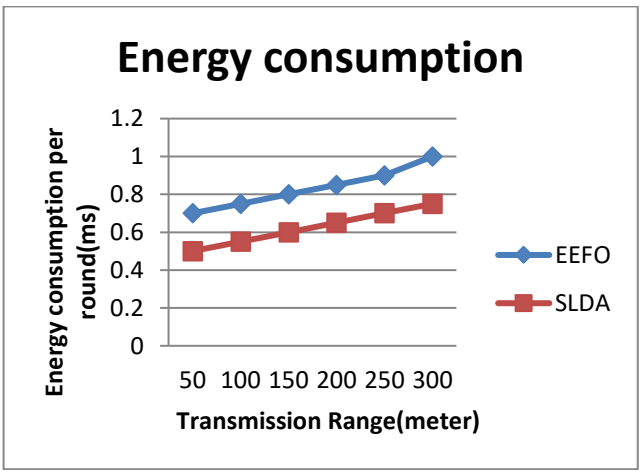

Figure 3: Transmission range vs. energy consumption

The fig.4 shows that attack is reduced in SLDA when compared to EEFO because it takes the aggregation based deviation but where as in SLDA, deviation is not considered for aggregation.

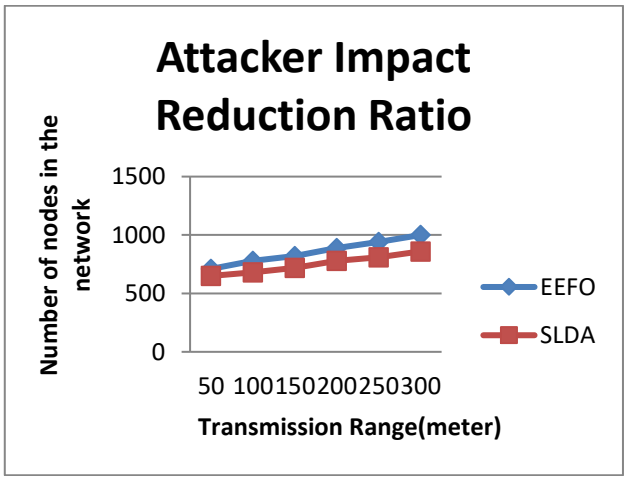

Figure 4: Attacker impact reduction ratio

The fig.5 shows that Overhead of SLDA is reduced when compared to EEFO because of using constructive acknowledgement scheme. Overhead is increased when nodes are increasing. To avoiding overheard it uses optimal path for forwarding data to the destination.

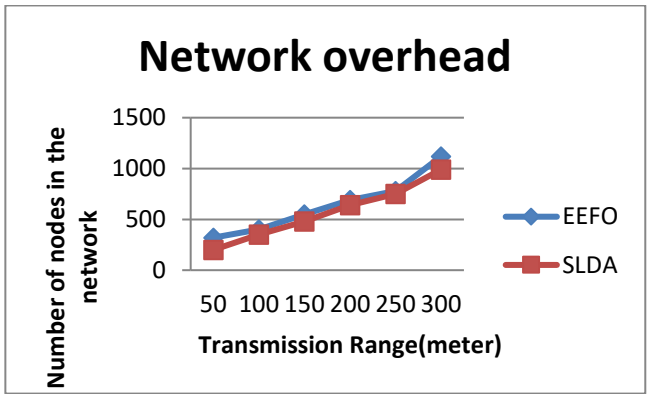

Figure 5: Overhead in the network

5. Conclusion

In this paper, it uses the three methods for secured data aggregation and also analysis the performances of parameter metrics. It consider the parameters energy consumption , overhead, network lifetime and attack impact reduction ratio for detective and avoiding the malicious nodes in the networks. After compared with other algorithms SLDA is more efficient secured data transmission method. This method further improved by increasing number of nodes and more energy efficient. In this paper compared to other metrics, the overhead reduced in this work is more over same as EEFO method. So, In future it will concentrate on reducing network overhead.

References

[1] Zhu W, Xiang Y & Zhou J, "Secure localization with attack detection in wireless sensor networks", *International Journal of Information Security*, Vol.10, No.3, (2011), pp.155-171.

[2] Roy S, Conti M, Setia S & Jajodia S, "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact", *IEEE Transactions on Information Forensics and Security*, Vol.9, No.4, (2014), pp.681-694.

[3] Kavitha T & Sridharan D, "Security vulnerabilities in Wireless Sensor Networks: A survey", *Journal of Information Assurance and Security*, Vol.5, (2010), pp.31-44.

[4] Balamurugan P, "Geometric Designs for Energy and Delay Computing for Data Gathering in Wireless Sensor Networks", *journal of current computer science and technology*, Vol.5, No.5, (2015), pp.31-38.

[5] Sadek AK, Yu W & Liu KJR, "On the energy efficiency of cooperative communications in wireless sensor networks", *ACM Transactions on Sensor Networks*, Vol.6, No.1, (2009).

[6] Jacobs IS & Bean CP, "Fine particles, thin films and exchange anisotropy", *Magnetism*, Vol.III, (1963), pp.271–350.

[7] Pradeepa K, Anne WR & Duraisamy S, "Design and implementation issues of clustering in Wireless Sensor Networks", *International Journal of Computer Applications*, Vol.47, No.11, (2012), pp.23-28.

[8] Alcaraz C, Lopez J & Roman R, "Selecting Key Management Schemes for Wireless Sensor Networks application", *Journal of Computers and Security*, Vol.31, No.8, (2012), pp.956-966.

[9] Azarderskhsh R & Reyhani A, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks", *Eurasip Journal on Wireless Communications and Networking*, (2011), pp.1-12

[10] Chan AC & Castelluccia C, "A security framework for privacy preserving data aggregation in wireless sensor networks", *ACM Transactions on Sensor Networks*, Vol.7, No.4, (2011), pp.29-35.

[11] Chatterjea S & Havinga P, "A Dynamic data aggregation scheme for Wireless Sensor Networks", *Proc. ProRISC*, (2003), pp.56-60.

[12] Dietrich I & Dressler F, "On the lifetime of wireless sensor networks", *ACM Transactions on Sensor Networks*, Vol.5, No.1, (2009).

[13] Kalpakis K, Dasgupta K & Namjoshi P, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks", *Computer Networks*, Vol.42, No.6, (2003), pp.697-716.

[14] Xue Y, Cui Y & Nahrstedt K, "Maximizing lifetime for data aggregation in wireless sensor networks", *ACM/Kluwer Mobile Networks and Applications (MONET) Special Issue on Energy Constraints and Lifetime Performance in Wireless Sensor Networks*, (2005), pp.853-864.

[15] Hong B & Prasanna VK, "Optimizing system lifetime for data gathering in networked sensor systems", *Workshop on Algorithms for Wireless and Ad-hoc Networks*, (2004).

[16] Padmaja P & Marutheswar GV, "Secured Data Aggregation In Wireless Sensor Networks", *International Journal of Applied Engineering Research*, Vol.11, No.7, (2016), pp.4740-4745.

[17] Padmaja P & Marutheswar GV, "Optimization of Wireless Sensor Networks in Secured Data Aggregation", *International Journal of Electrical and Electron is Engineering Research*, Vol.7, No.2, (2016), pp.94-100.