An Efficient Weighted Trust Method for Malicious Node Detection in Clustered Wireless Sensor Networks

Bhavnesh Jaint
Department of Electrical Engineering
Delhi Technological University
Delhi, India
bhavneshmk@gmail.com

Vishwamitra Singh
Department of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
vishwamitra_bt2k15@dtu.ac.in

Lalit Kumar Tanwar
Department of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
lalittanwar55@yahoo.com

S.Indu
Department of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
s.indu@dce.ac.in

Neeta Pandey
Department of Electronics and Communication Engineering
Delhi Technological University
Delhi, India
neetapandey@dce.ac.in

***Abstract*—In this paper, we consider a wireless sensor network (WSN) that consists of sensor nodes (SN), cluster head (CH), forward node (FN) and a base station (BS). The information acquired by the sensor node is sent to the CH, all the CH's send the information to a FN which forwards it to the BS. Fast detection of malicious nodes is imperative to the performance of a WSN and therefore we study the weighted trust method for malicious node detection. We have considered two scenarios one with single cluster head without grid and other with multiple cluster head with non-overlapping grid. The results indicates that the scenario with multiple cluster heads with non-overlapping grid requires less time for malicious node detection with better accuracy as compared to the scenario with single cluster head without grid.**

***Keywords*—weighted trust, sensor nodes, malicious nodes, cluster cased WSN,**

I. INTRODUCTION

Wireless Sensor Network (WSN) have a huge domain in applications varying from emergency response system, energy management, medical monitoring, logistics management, inventory management, and battlefield management [11]. WSN consists of a group of small devices which are called sensor nodes. These nodes are portable devices equipped with sensors, processing unit, memory unit, transceiver and power supply as shown in Fig.1. The sensor nodes are application specific and are intended to monitor specific parameters like temperature, pollutant levels at various locations, particle concentration in chemicals, pressure, intensity of sound/light, etc. These sensors are deployed randomly in a geographical region of interest. The sensor nodes collects information and send it to base station (BS) with the help of cluster head (CH) node and forward node (FN). The sensor nodes have limited power supply, usually a battery and therefore possess limited capabilities. The forwarding nodes are assumed to have high power and it collects and processes the data from lower level sensor nodes (SNs) and Base Stations (BSs) that act as media between Wireless Sensor Network (WSN) and wired network. The clusters are formed by equipartitioning the area under operation in four clusters. Each cluster head processes the data from all sensor points under it and pass the result to forwarding node. This scheme is based on assumptions that the forwarding node and base stations are not malicious and thus are always trusted.

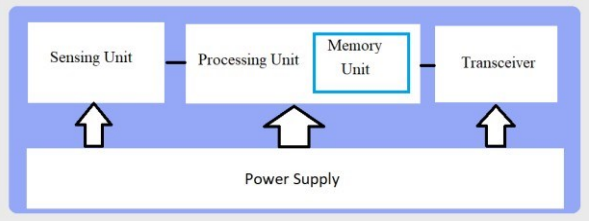

Figure 1. WSN Sensor Node Components

Due to unattended nature of the sensor networks, an attacker could launch various attacks and compromise sensor nodes. The network should be robust against these attacks, and if an attack succeeds, its impact should be minimized. Compromising of one or few sensor node should not crash the entire network. Therefore the critical issues of security and performance have to be studied for wireless sensor networks.

There have been many techniques presented in literature for detection of malicious node in wireless sensor networks.

There have been many techniques presented in literature for detection of malicious node in the wireless sensor networks. Wireless Sensor Networks can be compromised due to many reasons such as finite battery life, finite memory space, and finite computing capabilities [1], [2], [3]. It is very essential to detect the malicious node and isolate it to prevent it from generating wrong results. Ad hoc networks without a definite structure are rarely good against any types of attacks, which can lead to a node being compromised easily [4]. They presented a method that if a node is treated as trusty by its neighboring, then the node will be declared fault free, and is not a malicious node. However, for it to work it must have a minimum number of nodes nearby, which is not guaranteed in sensor networks.

So the better idea as proposed by W. Du, L. Fang and P. Ning [6] to get the node to compare the data from the other nodes nearby around it with the data generated by the node itself. If the difference between the data is marginal, then the nodes are said to be trusty. This method gave a better result for the localized detection of malicious node.

978-1-5386-6625-8/18/$31.00 ©2018 IEEE

Weighted Trust Evaluation, used primarily for the detection of the malicious node is quite reliable. The entire sensor nodes are assigned a weight or amount of trust that is evaluated frequently. The trust decreasing every time the node provides wrong information. Once the trust decreases below the fixed threshold, the node is declared malicious and isolated [5] [7] [8] demonstrated the method by using a three-level hierarchical network with components as: Sensor Nodes (SN) whose function is to sense the parameter. SNs sends its data to Forwarding Node. Forwarding nodes are high powered that collects data from SNs and processes it and transmits to base station.

This scheme is based on one critical assumption, the forwarding nodes and Base station are never faulty as once a faulty forwarding node is entered it can launch attack in network [9] [10] [7]. [15] Presents extensive simulation in MATLAB for Extensive weighted trust evaluation emphasizing on response time and detection ratio [13] [14]. Focused on the security issues in WSN and described the various kinds of attacks [17] described various clustering algorithms in the network, these clustering algorithms describes a power efficient way to localize sensor nodes and increase reliability.

In this paper we study the propagation time required to detect the malicious sensor nodes using weighted trust evaluation scheme. We compare the time taken by a traditional weighted trust evaluation scheme [5] (one with three level hierarchical network consisting of Sensor Nodes, Forwarding Node and Base Stations) with time taken by one proposed cluster based weighted trust evaluation (one with hybrid topology sensing nodes, cluster head, forward node and base station).

The rest of the paper is organized as follows. Section II describes the security in WSN and related work. Network model and architecture to be used throughout the paper is presented in Section III. In Section IV Cluster based weighted trust evaluation scheme is presented. Simulation results are shown in Section V. This paper concludes in Section VI.

II. Security in WSN

Security in WSN is paramount importance and the following are the challenges faced while designing WSN:

Unfavorable harsh environment: Sensor nodes faces extremely harsh environmental conditions and are susceptible to damage through it or capture by attackers as the sensor nodes are exposed in an open area. The attackers can capture a sensor node and access to data or transmit false data through them.

Unattended operations: The sensor nodes are deployed in a hostile area which expose them to physical tempering and attacks.

Limited resources: The security of sensor nodes requires resources like energy, memory and storage capacity as the data are constantly monitored and/or recorded the shortage of resources of sensors brings out challenges to resource-intensive security mechanisms. These resources are very limited in a small sensor node.

Reliability in Wireless Communication: In WSN the sensor data may be distorted due to channel errors which may lead to conflicts, and at highly busy node the data may also be and thus Denial-of Service (DoS) attack can be easily launched. Due to the greater congestion at a single node the overload results in increasing the latency in the sensor network thus causing synchronization errors and lag in the system, including sensor nodes. Attackers can launch an attack in sensor network through malicious nodes. These attacks are broadly classified as Passive attack and Active attack. The passive attack is easier to analyze and is difficult to detect. In passive attack, attacker does not modify or exchange information, this type of attack is basically for finding the knowledge of some classified information [12].

In an active attack the attacker tries to alter the data transferred by the sensor node or overload the sensor by inserting the traffic to start denial of service attack.

III. Network Model And Architecture

There are basically two components of network model i.e. WSN components and WSN networking topology. The components are explained as follows:

A. Components of WSN

Wireless Senor Network for environment monitoring for air pollution system consists of the sensor points or sensor nodes that are spread over the field. These sensor nodes consist of sensors that detects and monitors the concentration of pollutants in the environment. These sensor nodes are connected together through a wireless link to the cluster head that processes the collected readings from every individual node and forwards these data to the forwarding node that again processes the collected readings from individual cluster heads and propagates it to a base station shown in Fig.2.

B. Network Topology

In Wireless Sensor Network we present a clustered WSN architecture that uses a hybrid network topology which combines star, mesh and ring topologies together. These three topologies are used to increase the versatility of the system while maintaining reliability taking into account the available resources as following [16]:

- A group of the sensing nodes are connected to a central node i.e. cluster head that has other abilities like connectivity and data exchange from other cluster heads this includes the star topology thus resulting is a set of clusters. Star topology has advantages over other topologies that includes its scalability and power usage reduction.
- Cluster heads are connected together as a mesh to provide a reliable communication, clusters heads had additional resources that facilitate the use of such topology. All clusters heads are connected directly to the forwarding node which acts as a path from wireless to wired network i.e. to the outside world. Fig.2 depicts the overall architecture of WSN using hybrid network topology.

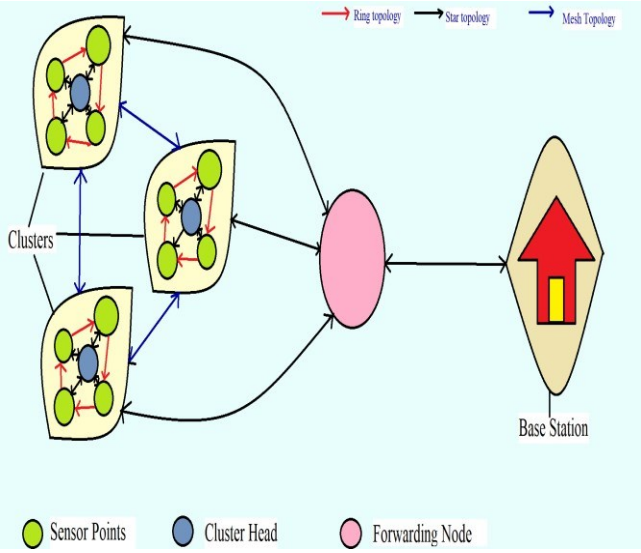

Figure 2. System Architecture

C. Error Detection and Weight Reduction Formula

In detecting malicious nodes, we employ trust values of sensor node to reflect their track record in decision making process. Each cluster head maintains trust values of its associated sensor nodes. The trust value (V_w) lies in the range (0,1) and is initialized to 1 for each sensor node. The weight represents the sensor node dependability and the sensor node with a higher weight is more trustworthy. Updating the trust values is important to maintain the fidelity of the readings obtained from the sensors. To determine the non-erroneous node the weighted threshold value should be greater than the minimum threshold value.

$$V_{th} \leq V_w$$

$$V_w = \frac{M - |D|}{M}$$

Where, V_{th} is the minimum threshold weight and V_w is the weighted threshold. M is the Average or mean value of the sensor at a point. (M is the user defined value). D is the deviation from the M. D is dependent on sensor input value and can be calculated as ($M - I$). Where I is the Input value from the sensor.

For example in a tropical rainforest thee temperature varies from 21 to 30 degrees then the value of mean (M) would be 25.5 degrees. If a particular sensor detects the temperature at that time the detected value would be I. Let the detected value be 34 degrees. Now the calculated threshold value would be

$$V_w = \frac{25.5 - |25.5 - 34|}{25.5}$$

Thus, V_w is calculated to be 0.67. Assuming the minimum threshold to be set to 0.7, the equation $V_{th} \leq V_w$ is not satisfied. Thus the corresponding sensor node is an erroneous node.

Weight Modification

If the sensor node is found as erroneous then the weight is reduced according to following formula.

$$W' = W + F \times W$$

Where W' Is the modified weight, W is the current weight and F is weight penalty factor.

IV. Cluster Based Weighted Trust Evaluation

The goal was to come up with a prototype of the enhanced weighted trust evaluation scheme that detect malicious Sensor Nodes and Cluster Heads. The performance requirements that the scheme should meet are short response time, high detection ratio and low misdetection ratio. Response time refers to the average number of cycles required by the scheme to correctly detect malicious nodes, detection ratio refers to the ratio of malicious nodes correctly detected by the scheme to the total number of malicious sensor nodes present in the WSN. Several sensor nodes "n" are deployed randomly in the field, a subset of them are elected as the forwarding nodes whereas the rest become the ordinary sensor node (SN). The sensor nodes organize themselves to form a clustered operational network.

V. Simulation Results

The WTE based detection algorithm was installed in the cluster node for monitoring of all the member sensor nodes.

TABLE I. Simulation Parameters

Minimum threshold weight	0.7
Number of clusters	4
Number of repetitions of samples	5
Network field dimension	100x100
Sensor Nodes in field	100
Weight Penalty Factor	20%
Malicious nodes at deployment	20%

Though the field parameters are user inputs but heterogeneous network of hundred sensor nodes are deployed randomly in the area with a dimension of [100x100] the simulation is as shown in Fig.4

The Sensors are grouped in clusters and the weighted trust evaluation algorithm performs over it. As shown in figure 5 the malicious nodes are displayed in respective clusters. This method is performed for 5 times and the propagation time is compared in figure 6. It is shown that the propagation time decreases with clustering and increases without clustering as the number of samples increases.

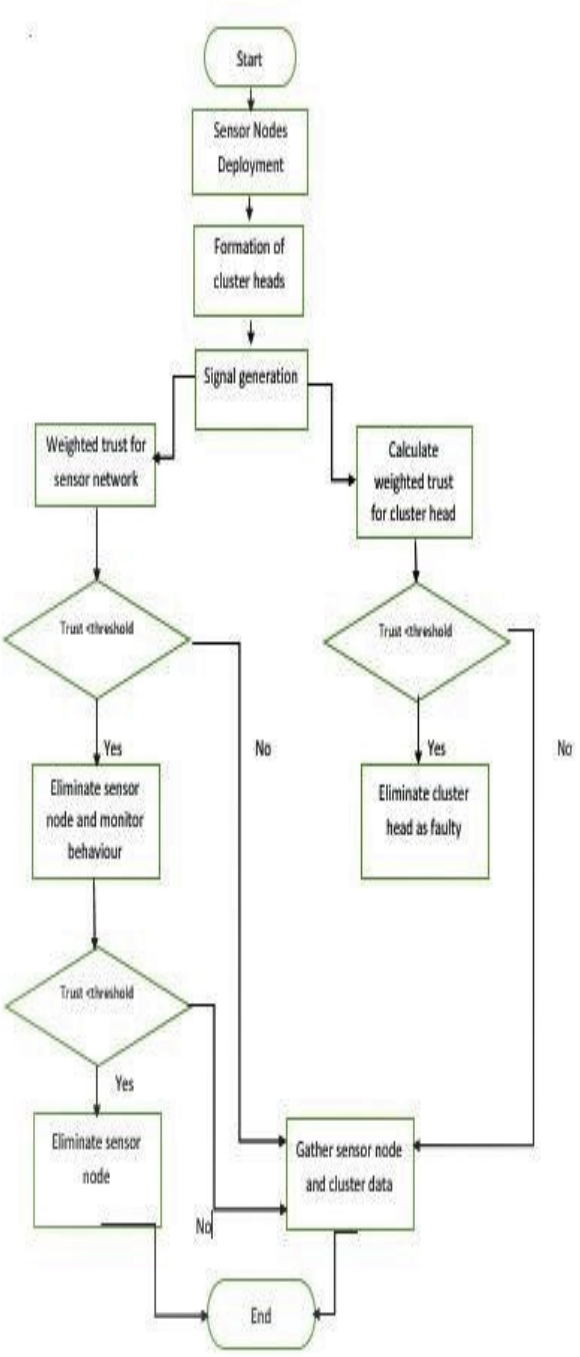

Figure 3. Algorithm for Weighted Trust Evaluation

Though the field parameters are user inputs but heterogeneous network of hundred sensor nodes are deployed randomly in the area with a dimension of [100x100] the simulation is as shown in Fig.4

The Sensors are grouped in clusters and the weighted trust evaluation algorithm performs over it. As shown in figure 5 the malicious nodes are displayed in respective clusters. This method is performed for 5 times and the propagation time is compared in figure 6. It is shown that the propagation time decreases with clustering and increases without clustering as the number of samples increases.

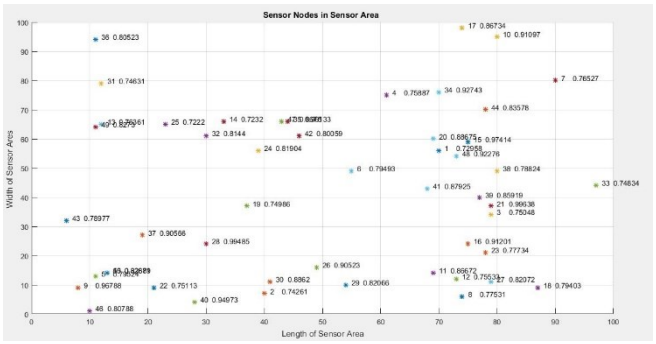

Figure 4. Plot of all the Sensor Nodes in an area

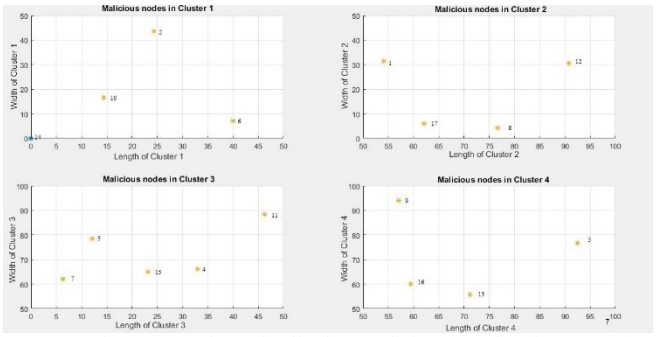

Figure 5. Plot of all the Malicious Nodes in respective forwarding node

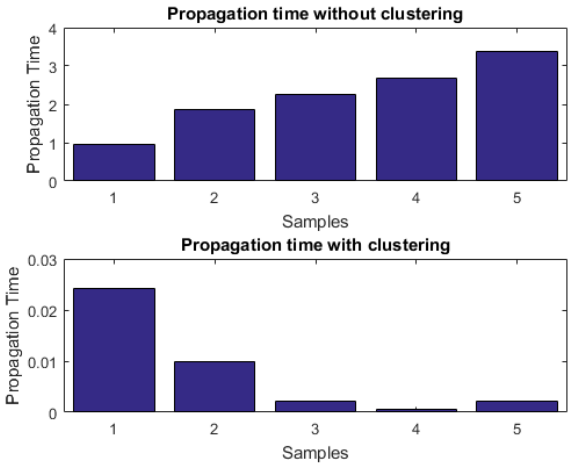

Figure 6. Time taken to find malicious nodes in

i. Whole area at once and then find propagation time.
ii. Considering individual clusters and then find propagation time including all forwarding nodes.

Detection Ratio:

Detection Ratio (DR) is the ratio between the number of malicious nodes detected and the total number of malicious nodes in the network (set at the time of deployment). In one of the simulation runs, the percentage of malicious nodes, is set to 20% (m = 0.2). This means that:

Malicious nodes = 20/100 * n

Where n = number of deployed sensor nodes i.e. =100.

Malicious nodes =20

There is one more set of malicious nodes that is cluster head

Malicious cluster head = m *(p*n)

=20/100 *(4/100 * 100) = 0.8=1

Where p= percentage of cluster head in the network =4/100.

TABLE II. Parameter Vs Nodes

Total Malicious Nodes (At Deployment)	20	40	60	80
Detected Malicious Nodes (Simulation)	18	33	38	29
Detection Ratio (DR)	0.9	0.83	0.63	0.36

Malicious ordinary sensor nodes = m *(n- (p*n))
=20/100 * (100 – (4/100* 100)) = 19.2= 19
The number of detected malicious ordinary sensor nodes is 17 out of the 19 (Through Simulation) that had been set as malicious whereas all the malicious cluster heads are detected by the method.
Detection Ratio = No. of correctly detected malicious nodes/Total no. of malicious nodes in the network.
DR = (17 + 1) / 20 = 0.90
In figure 7, we plot the number of malicious nodes vs detection ratio. It is observed that the detection ratio decreases with the increase in malicious nodes.

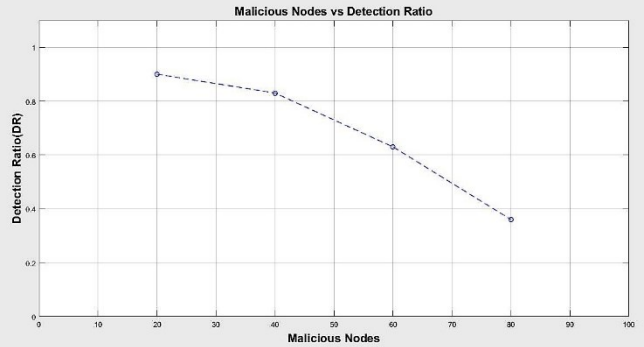

Figure 7. Malicious Nodes vs Detection Ratio

VI. CONCLUSION

The simulation clearly shows that the propagation time in second case (when individual clusters are considered independently instead of whole area at once) is much smaller (nearly1times less).Also 90% malicious nodes are detected when 20 malicious nodes at deployment are considered. If the number of clusters are increased then the Detection Ratio would increase.

In this paper simulation results are being reported and they shows that algorithm can be applied to a flexible number of sensor nodes that operate under a cluster head, it thus has achieved better scalability with a considerable detection rate and less propagation time.

REFERENCES

[1] E. Ayday, F. Delgosha, and F. Fekri, “Location-Aware Security Services for Wireless Sensor Networks using Network Coding,” *Infocom*, May 2007.

[2] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” *CCS'03*, October 2003.

[3] C. Karlof, N. Sastry, and D. Wagner, “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks,” *ACM Sensys*, November 2004.

[4] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, “Self-securing Ad Hoc Wireless Networks,” IEEE ISCC (IEEE Symposium on Computers and Communications) 2002, Italy.

[5] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku and Zhou Su, "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", SpringSem, pp. 836-843, 2008.

[6] W. Du, L. Fang, and P. Ning, “LAD: Localization Anomaly Detection for Wireless Sensor Networks,” the 19th International Parallel and Distributed Priocessing Symposium (IPDPS’05), April 3 – 8, 2005, Denver, Colorado, USA.

[7] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku and Z. Su, Malicious Node Detection in Wireless Sensor Networks, The Symposium on Simulation of Systems Security (SSSS‟08), Ottawa, Canada, p. 838, 2008.

[8] S. Zhao, K. Tepe, I. Seskar and D. Raychaudhuri, Routing Protocols for Self-Organizing Hierarchical Ad-Hoc Wireless Networks, Proceedings of the IEEE Sarnoff Symposium, Trenton, NJ,, March 2013.

[9] K. Sumathi and D. M. Venkatesan, A Survey on Detecting Compromised Nodes in Wireless Sensor Networks, (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, pp. 7720-7722, 2014.H. Hu, Y. Chen, W.-S. Ku, Z. Su and C.-H. J. Chen, Weighted trust evaluation-based malicious node detection for wireless sensor networks, Int. J. Information and Computer Security, vol. 3, no. 2, p. 148, 2009.

[10] R. Sharma and N. Tripathi, Comprehensive Review on Wireless Sensor Networks, Oriental Journal of Computer Science & Technology, Vol. 8, No. 1, pp. 59-64, April 2015.

[11] D. G. Padmavathi and M. D. Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, International Journal of Computer Science and Information Security,, vol. 4, 2009.

[12] Rajkumar, Vani B. A., G. Rajaraman, Dr. H. G. Chandrakanth, “Security Attacks and its Countermeasures in Wireless Sensor Networks”, Int. Journal of Engineering Research and Applications, Vol. 4, Issue 10 (Part-1), pp. 04-15, October 2014.

[13] Mohamed-Lamine Messai” Classification of Attacks in Wireless Sensor Networks” International Congress on Telecommunication and Application’14University of A.MIRA Bejaia, Algeria, 23-24 APRIL 2014.

[14] Koriata P. Tuyaa and W.Okelo-Odongo, “Enhanced weighted Trust Scheme for detection of malicious nodes in Wireless Sensor Networks”, International journal of computer applications (0975-8777), Vol 155-No.4, December 2016.

[15] T. Sathyamoorthi, D. Vijayachakaravarthy, R. Divya And M. Nandhini, A Simple and Effective Scheme To Find Malicious Node In Wireless Sensor Network, International Journal of Research In Engineering And Technology, Vol. 03, No. 02, 2014.

[16] X. liu and J. Shi, “Clustering Routing Algorithms in Wireless Sensor networks: an overview”,KSII Transactions on Internet and Information Systems, Vol 6, No.7, 2012 :pp.1735-1755.