ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Distributed Detection of Malicious Node in Wireless Sensor Network under Byzantine Attack Strategies

Jayanti Pandey, Dr. Achala Deshmukh

Department of Electronics & Telecommunication, Sinhgad College of Engineering, Pune, India

Department of Electronics & Telecommunication, Sinhgad College of Engineering, Pune, India

ABSTRACT: Wireless sensors network (WSN) are setup in environment where sensors can be exposed to circumstances that might interfere with measurement provided. Distributed detection is used which overcome sensors failure and coverage problem in mobile access wireless sensor network under Byzantine attacks. Power consumption is always a problem in wireless sensor network. There must be less energy consumption to improve the quality of service of sensor network. The packet delivery should be reliable and scalable for the wireless sensor network for performing and better point of view. In Byzantine attacks, compromised sensors send false sensing data to base station, leading to increased false alarm rate. There are different attacking strategies which can be adopted by byzantine attack to disrupt the network. However due to high computational complexity of the optimal scheme parameters for hard decision rule, therefore this rule is infeasible as network size increase and/or the attack behaviour changes. Proposed system focus on detection of malicious node is done under time-varying attacks. The objective of the work proposes to study the security aspects of WSNs, considering the Distributed Detection of Byzantine Attacks. The response of network parameters i.e. throughput, energy consumption, control-overheads etc. are recorded under Byzantine attack.

KEYWORDS: Wireless Sensor Networks, Byzantine attacks, Malicious node.

I. INTRODUCTION

Wireless Sensor Network

Wireless sensor networks consist of very small devices, called sensor nodes, that are battery powered and are equipped with integrated sensors, a data-processing unit, a small storage memory, and short-range radio communication. Typically, these sensors are randomly deployed in the field. They form an unattended wireless network, collect data from the field, partially aggregate them, and send them to a sink that is responsible for data fusion. Sensor networks have applications in emergency-response networks, energy management, medical monitoring, logistics and inventory management, and battlefield management. In contrast to traditional wireless networks, special security and performance issues have to be carefully considered for sensor networks. For example, due to the unattended nature of sensor networks, an attacker could launch various attacks and even compromise sensor devices without being detected. Therefore, a sensor network should be robust against attacks, and if an attack succeeds, its impact should be minimized. In other words, compromising a single sensor node or few sensor nodes should not crash the entire network. Another concern is about energy efficiency. In a WSN, each sensor node may need to support multiple communication models including unicast, multicast, and broadcast. Therefore, due to the limited battery lifetime, security mechanisms for sensor networks must be energy efficient. Especially, the number of message transmissions and the amount of expensive computation should be as few as possible. In fact, there are a numbers of attacks an attacker can launch against a wireless sensor network once a certain number of sensor nodes have been compromised. In literature, for instance, HELLO flooding attacks, sink-hole attacks, Sybil attack, black hole attack and wormhole attacks are options for an attacker.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Byzantine Attack

A serious threat to wireless sensor networks is the Byzantine attack, where the adversary has full control over some of the authenticated nodes and can perform arbitrary behaviour to disrupt the system. Byzantine fault encompasses both omission failures as failing to receive a request, or failing to send a response and commission failures as processing a request incorrectly. Byzantine attacks are such attacks where it expose with the set of intermediate nodes that working individual within the network carry out attacks like forming routing loops, consuming time and bandwidth by forwarding packet from non-optimal paths, selective dropping of packets which disrupt the network. Many byzantine attacks contribute some feature of selfish node, these nodes immediately affects the self-operation of nodes and do not intercept in performance of network. These nodes purposely drop thepacket in order to conserve the resources. In wireless sensor network byzantine attack has following types concerned with nodes: Selfish-node attack, Black Hole attack, Wormhole attack, Gray Hole attack.

Features of Byzantine attack are as follows:
• Directing circles within the nodes with no definite ends.
• Sending parcel through non-ideal way.
• Specifically dropping of packets.

Selfish Node Attack :
Selfish node attack is one such attack in which a faulty node performs routing misbehaviour in the route discovery packets to advertise itself as having the shortest path to the node whose packets he want to compromise. The attacker aims at modifying the information so that they can control the traffic flow of the network. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find new path to destination. Malicious nodes quickly respond to the source node as these nodes do not refer the routing table and drop all the routing packets and also flooding the false information of shortest route in network by that the number of nodes that are in radio range directly or indirectly forwarded the routing as well as data packets in the network. The source node assumes that the route discovery process is complete and ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets.

Black hole attack:
In this attack, when a malicious node sense some route request packet in the network, it reply the legitimate node by pretending that it has shortest and original route to the destination node even if no such fair route exists. As a result, the vicious nodes easily drop the packet or mislead the routing information in the network which is utilized for forwarding the packets. 1.2.3. Gray-hole attack It is peculiar type of black hole attack where gray hole is carried, which drops selective packets such as forwarding packets but not data packet. 1.2.4. Worm-hole attack Worm hole connects two different points in space through shortcut path. In this attack a pair of attacking nodes can intercept the route by short circuiting the network. Wormhole attack can be performed with single node too but generally it is carried out by wormhole link.

Motivation

The wireless sensors then can be made of low cost devices adhering to the severe constraints on battery power. But, this requires that such practical limitations make use of sophisticated encryption, which eventually makes it more unrealistic. The wireless transmission medium is more vulnerable to eavesdropping and packet dropping, which makes it possible for the attacker to extract information from sensor transmissions. As a result, the adversary can employ a wide range of strategies, including deploying its own sensors aimed at jamming the transmission of honest sensors or, in a more sophisticated way, transmitting optimally designed signals to confuse the transmitting nodes.
• Distributed detection, effectively reduce the volume of data transmission in network.
• Improve Bandwidth utilization.
• Reduce total network traffic in a wireless sensor network
• The Byzantine sensor problem is motivated by applications of envisioned wireless sensor networks where sensors are more vulnerable to tampering.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Problem Statement

Here the classical problem of distributed detection but under the assumption that some of the sensors have been compromised by an intruder. The compromised sensors are referred to as Byzantine and they can be reprogrammed by the intruder to attack the transmitting node by transmitting fictitious data. The rest of the sensors are referred to as honest, and they follow the expected rule of operation. In going research it is obtained that the optimal scheme parameter can only be obtained through exhaustive search, making it infeasible for large networks.

II. BACKGROUND AND RELATEDWORK

In [1], proposed system has considered distributed detection in the presence of Byzantine sensors created by an intruder, and characterized the power of attack analytically. They are able to provide closed-form expressions for the worst detection error exponent of an optimized NP detector at the fusion centre, and for the corresponding attacking distributions. In [2], they considered the q-out-of-m fusion rule for SENMA networks under Byzantine attacks. Both static and dynamic attack strategies were discussed. The proposed work simplified q-out-of-m fusion schemes by exploiting the linear relationship between the scheme parameters and the network size. They also derived a near-optimal closed-form solution for the fusion threshold based on the central limit theorem. An important observation is that, even if the percentage of malicious sensors remains fixed, the false alarm rate diminishes exponentially with the network size. This implies that for a fixed percentage of malicious nodes, which can improve the network performance significantly by increasing the density of the nodes. Furthermore, they obtained an upper bound on the percentage of malicious nodes that can be tolerated using the q-out-of-m rule. It is found that the upper bound is determined by the sensors‘detection probability and the attack strategies of the malicious nodes. Finally, proposed an effective malicious node detection scheme for adaptive data fusion under time-varying attacks. The detection procedure is analyzed using the entropy-defined trust model, and has shown to be optimal from the information theory point of view. It is observed that nodes launching dynamic attacks take longer time and more complex procedures to be detected as compared to those conducting static attacks. The adaptive fusion procedure has shown to provide significant improvement in the system performance under both static and dynamic attacks. Further research can be conducted on adaptive detection under Byzantine attacks with soft decision reports.

In [3], proposed system introduced a robust and efficient security mechanism for delay tolerant networks. The proposed security mechanism consists of a trust management mechanism and an iterative trust and reputation mechanism (ITRM). The trust management mechanism enables each network node to determine the trustworthiness of the nodes that it had a direct transaction. On the other hand, ITRM takes advantage of an iterative mechanism to detect and isolate the malicious nodes from the network in a short time. This scheme is far more effective than the voting-based techniques in detecting Byzantine nodes. Routing, QoS provisioning, energy efficiency, security and multicasting are challenges in WSN. As security is not a product, it is a process, system originator should maintain up to-date with the progresses in attacks on embedded systems. The security of significant systems should be continually reassessed to take new detections into account. The level of security needed from the application should also be marked when preferring hardware. At someindefinite time it might reasonable to put up additional protection, for instance a secure place, around a vulnerable microcontroller. In [5], they developed a coding scheme which provides strong secrecy by combining nested lattice codes and universal hash functions. Here, they showed that the same theorem is also useful in bounding another information-theoretic measure, which in turn leads to the desired strong secrecy results in a Gaussian setting. They showed that this coding scheme can be used with AMD codes to perform Byzantine detection for a Gaussian two-hop network where the relay is both an eavesdropper and a Byzantine attacker. Using this code, they showed that the probability that a Byzantine adversary wins decreases exponentially fast with respect to the number of channel uses. It should be noted that, in this paper, they have assumed that the channel gains are known by each node before the communication starts. It should be recognized that the Byzantine attacker at the relay node may attempt to manipulate the channel estimation process, for example, by broadcasting incorrect pilot signals, to gain an advantage. Detection of this type of misbehaviour is closely related to the physical layer implementation of the system. In existing work on event detection for wireless sensor networks, most of them are based on the simplifying assumptions that there is perfect Channel State Information (CSI) between the sensors and the gateway (GW). In addition, they have not

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

considered the effect of malicious nodes on the system performance. In [6], a novel algorithm based on a statistical approach is developed and model the Byzantine attack function in order to accurately detect the occurrence of events in the face of such attacks and considered two practical cases where:1) channels between events and sensors have unknown CSI; 2) sensors transmit to GW with unknown CSI. They also formulate an optimal Byzantine attack function from the attacker‘s point of view. In this paper, system uses two distributed algorithms for these cases. Here develop the optimal event detection decision rule under Byzantine attacks for the first case and a novel low-complexity event detection algorithm based on Gaussian approximation and Moment Matching for the second case which considers a global decision.

III. SYSTEM MODEL

Trust Based Solution

Sensor nodes can monitor the behaviour of their neighbouring nodes and rate them. Assuming that an intruder drops all the packets, a intruder in such a system should have the least trust level and can be easily eliminated. A neighbouring node of a source node will have the highest trust level if all the packets sent reach the destination. In this method a base station observes the behaviour of the nodes and maintains the trust factor. The trust factor drops exponentially with each consecutive packet dropped which helps in detecting the malicious node. The method showed a drastic decrease in the number of packets dropped before the node being detected as a malicious node. Efficient and secure routing protocol is used to identify single and cooperative byzantine attack (black hole) in a self-motivated environment and thereby generates a secure routing path from source node to the destination node. This protocol encloses a feasible trust based solution that examines trustworthiness of neighbouring nodes. This approach keeps misbehaving nodes aside from being a part of a network communication process.

Malicious Node Detection

To improve the system parameters through malicious node detection, where the hostile behaviour is identified and the malicious sensors are discarded from the final decision making. First the source node transmits the route request to destination node. After receiving request from source node, destination node replies the node with the number of nodes which are participating in the transmission. Source node check whether the route replies is from destination node or not, if the address is matched then source node sends the data packet and maintains trust factor for them. If destination address is not matched, the source node alerts the base station. After that base station prepare blacklist of node and discard the entire blacklisted node from participating in further packet transmission.

Distributed Detection

The problem of Distributed Detection is limits the sensors to get compromised by an intruder. As a result, all the compromised sensors which refer to as Byzantine tend to get reprogrammed by the intruder to attack the FC by transmitting fictitious observations. The uncompromised sensors that are referred to as honest can then follow the expected rule of operation. But, in the context of distributed detection, sensors are more vulnerable to tampering due to the Byzantine Sensor problem which is particularly motivated by the applications of envisioned WSNs. However, the wireless sensors then can be made of low cost devices adhering to the severe constraints on battery power. But, this requires that such practical limitations to make use of sophisticated encryption which eventually makes it more unrealistic.

Path Construction Phase

During the first path discovery, the nodes discover the neighbour nodes to send the data packets and establish a route to sink node by transmitting the Route Request message and when the route is discovered, then the source node initiate the Route Reply message and create a new entry in neighbour routing table. In the second path discovery, the nodes participating in first path are not included in the second path routing. So, that there is establishment of second path between the source and the destination node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Routing Request of the First Path:
The source node sense the Surroundings area, collect the data and transmit the data to sink node by setting the transmit radius_d'. If the nodes with omni directional antennas are interested to find the sink node; the source node send flooded RREQ data packet to the surrounding nodes. RREQ packet consists of node ID, remaining energy of node and message ID of RREQ. The node firstly checks the message ID and searches the task table after receiving RREQ sent by other nodes, to ensure whether this RREQ is first received or not.

Routing Reply of the First Path:
After the selection of the routing table for the path, the destination node sets the transmit radius and send the RREP packet. The RREP packet contains receiver node ID number, sender node ID number, message ID number, and RREP signs so on. After receiving the RREP packet, the node first checks the data packet type whether it is RREP packet or not. If it is RREP packet, It checks the receiver node ID number, to check whether it is receiver node or not. If it is receiver node ID in the RREP, the node will check and records the message ID number, node ID and other node information and for next hop node, it will set the sender node ID and the RREP packet is transmitted.

Flow Chart:

In system implementation, first the network is created which is consisting of sensor nodes and base station. Source node sends route request message in the network with destination address. The nearest node receives the route request and check in the routing table for the destination node, if destination node address present in the routing table then request is transmitted to the destination node otherwise request is forwarded to nearest node. After receiving the route request, destination node send route reply to the source node. If malicious node is discovered during transmission an alert message is send to the base station. Base station prepares the list of malicious node and deletes them from the routing table.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

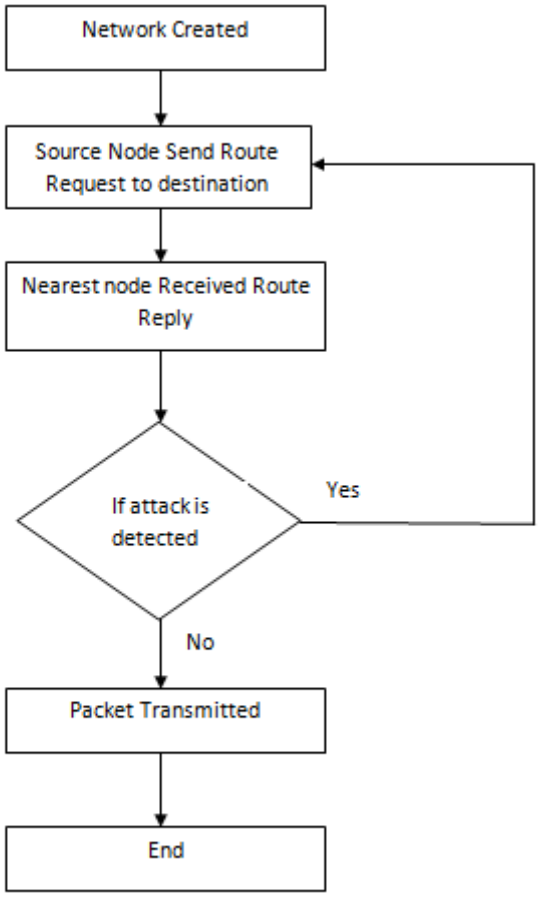

Figure. 01 System Implementation

Performance Parameter

a) Throughput: Throughput is defined as the rate of successful message delivery in a given time.

Throughput= packet size/Transmission time

b) Packet Delivery Ratio: Packet Delivery Ratio is characterized as the proportion of information packets got by the destinations to those dispatched by the sources.

PDR = Total no. of packets delivered / Total No. of packets dispatched.

c) End to end delay: End to end delay defined as the total time required reaching the packet from source to destination.

dend-end= N[dtrans+dprop+dproc+dqueue] where
dend-end= end-to-end delay dtrans= transmission delay
dprop= propagation delay dproc= processing delay
dqueue= Queuing delay N= number of links

d) Average energy consumption: Energy consumption is the ratio of the remaining energy provided by the available nodes to the total energy of nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

e) Normalized routing overheads: Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet.

IV. SIMULATION SETUP & RESULT

In this simulation 50 nodes are employed over the 1000m*1000m area. The two ray model is taken into consideration and traffic type used is CBR (constant bit rate). Simulation time is set to 200sec.

Table. Specification of simulation parameters

Parameters	Specification
No. of nodes	49
Base Station	1
Initial Energy of Nodes	100J
Routing Protocol	AODV
Traffic Type	CBR
Packet Size	512 kbps
Simulation time	200sec

Network Creation:

In wireless sensor network, energy model is one of the optional attributes of a node. The energy model denotes the level of energy in a mobile node. The components required for designing energy model includes initial-Energy, tx-Power, rx-Power, and idle Power. The ―initial Energy‖ represents the level of energy the node has at the initial stage of simulation. ―tx-Power‖ and ―rx-Power‖ denotes the energy consumed for transmitting and receiving the packets. If the node is a sensor, the energy model should include a special component called ―sense Power‖. It denotes the energy consumed during the sensing operation. Apart from these components, it is important to specify the communication range (RXThresh_) and sensing range of a node (CSThresh_). Base Station is configured with highest communication range. Data Transmission is established between nodes using UDP agent and CBR traffic.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

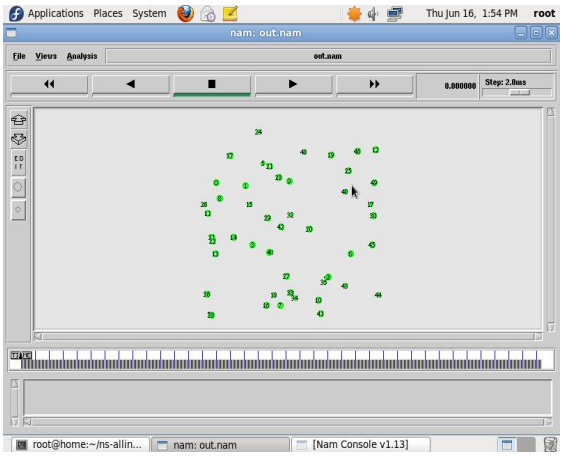

Figure. 02 GUI of Network

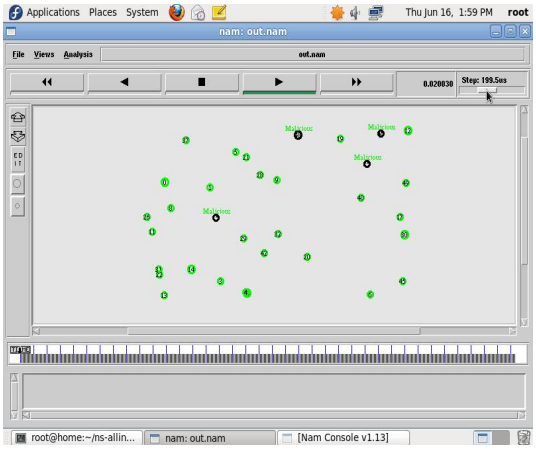

Figure. 03 Malicious node detected

Packet Delivery Ratio: Packet delivery ratio is characterized as the ratio of total number of packets received by the destination node to the total number of packets transmitted by the source node or Packet Delivery Ratio is characterized as the proportion of information packets got by the destinations to those dispatched by the sources. PDR = Total no. of packets delivered / Total No. of packets dispatched.

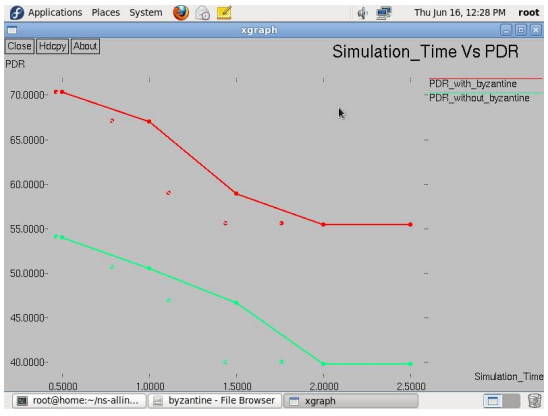

Figure. 04 Packet delivery ratio comparison

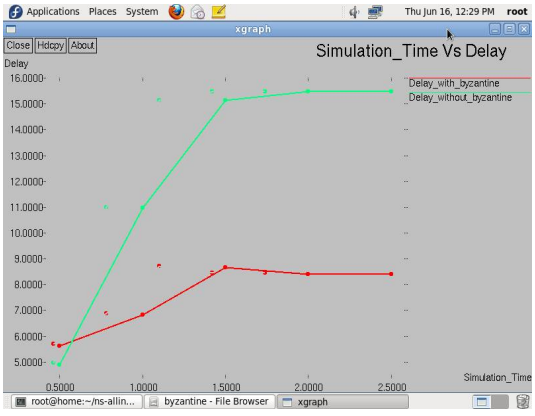

Figure. 05 End to End Delay

End to end delay defined as the total time required reaching the packet from source to destination.

dend-end= N[dtrans+dprop+dproc+dqueue]

Average energy consumption: Energy consumption is the ratio of the remaining energy provided by the available nodes to the total energy of nodes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

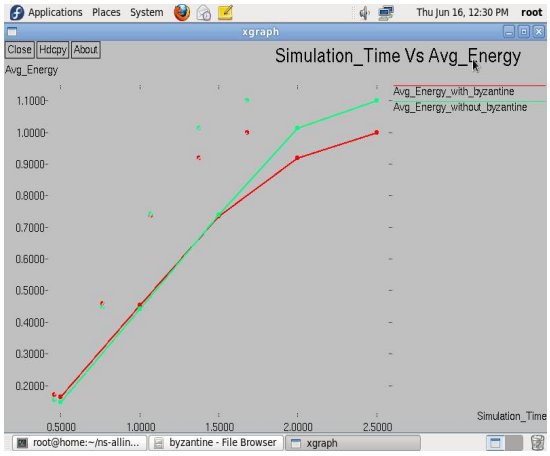

Figure. 06 Average energy consumption comparison

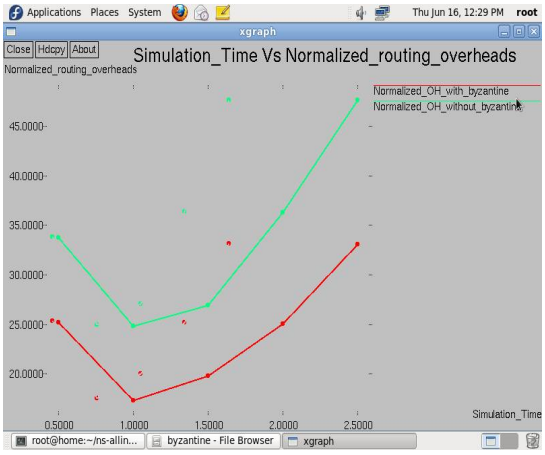

Figure. 07 Normalized routing Overheads comparison

Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet. It is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received. Protocol overhead refers to metadata and network routing information sent by an application, which uses a portion of the available bandwidth of a communications protocol. Nodes often change their location within network so, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

Throughput: Throughput is defined as the rate of successful message delivery in a given time. Throughput= packet size/Transmission time

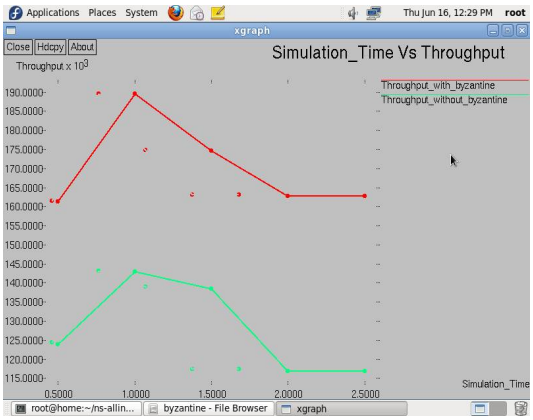

Figure. 08 Throughput comparisons

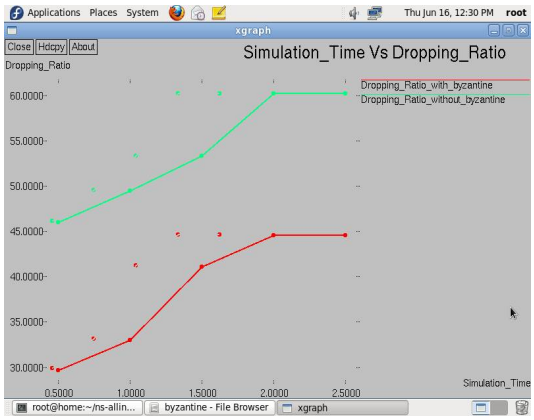

Figure. 09Dropping ratios Comparison

Dropping Ratio: It is ratio of packets lost during the transmission to the total packet transmitted.

V. CONCLUSION

The performance of the wireless sensor network is investigated under Byzantine attacks. The problems in distributed detection in wireless sensor networks are presented; an extensive literature survey on distributed detection of byzantine attack in wireless sensor network is summarized. The proposed work is as follows, first to design an experimental setup for detecting the malicious node in wireless sensor network. Second, trust- based solution is applied to the base station

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

and nodes to detect the byzantine attack. The response of the system parameters are compared with and without detection of the attack. With a very good scalability, our approach is applicable to both small size WSNs and WSNs with larger number of nodes. The only difference to apply it to larger size WSNs is to increase the number of Base Stations. The system performance is improved significantly after detection of Byzantine attack. The further examinations incorporate tests with high system traffic and interactive media information and on extensive geological zone, for example, city or significantly bigger environment. The detection accuracy of the proposed scheme is further investigated under static and dynamic attacking strategies.

REFERENCES

[1]. Stefano Marano, Vincenzo Matta, and Lang Tong, Fellow, ―Distributed Detection in the Presence of Byzantine Attacks,‖ IEEE Transactions on Signal processing, VOL. 57, NO. 1, January 2009.
[2]. Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren and Tongtong Li, ―Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks,‖ IEEE Transactions on Parallel and Distributed systems, vol. 25, no. 4, April 2014.
[3]. Erman Ayday, Hanseung Lee and Faramarz Fekri, ―Trust Management and Adversary Detection for Delay Tolerant Networks,‖ IEEE conference on Military communication, 2010.
[4]. Hero Modares, Rosli Salleh and Amirhossein Moravejosharieh, ―Overview of Security Issues in Wireless Sensor Networks,‖ IEEE Third International Conference on Computational Intelligence, Modelling & Simulation, 2011.
[5]. Xiang He, Member, IEEE, and Aylin Yener, Member, IEEE, ―Strong Secrecy and Reliable Byzantine Detection in the Presence of an Untrusted Relay,‖ IEEE Transactions on Information Theory, VOL. 59, NO. 1, January 2013.
[6]. Pengfei Zhang, Jing Yang Koh, Shaowei Lin and Ido Nevat, ―Distributed Event Detection under Byzantine Attack in Wireless Sensor Networks,‖ IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Symposium on Security, Privacy and Trust for Cyber-Physical Systems Singapore, 21–24 April 2014.
[7]. David Martins and Hervé Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms,‖ IEEE 13th International Conference on Network-Based Information Systems, 2010.
[8]. M. Abdelhakim, L. Lightfoot, and T. Li, ―Reliable data fusion in wireless sensor networks under Byzantine Attacks,‖ IEEE Military Communications Conference, November 2013.
[9]. S. Marano, V. Matta, and L. Tong, _Distributed detection in the presence of byzantine attack,‖ IEEE Transactions on Signal Processing, vol. 57, no. 1, pp. 16 –29, Jan. 2009.
[10]. A. Rawat, P. Anand, H. Chen, and P. Varshney, ―Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks,‖ Signal Processing, IEEE Transactions on, vol. 59, no. 2, pp. 774 – 786, Feb. 2011.
[11]. John S. Baras, Svetlana Radosavac, George Theodorakopoulos, Dan Sterne, Peter Budulas and Richard Gopaul, ―Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR,‖ IEEE, 2007.
[12]. S. M. Mishra, A. Sahai, R. W. Brodersen, ―Cooperative sensing among cognitive radios,‖ in Proc. IEEE ICC, 2006.
[13]. R. Chen, J. M. Park, K. Bian, ―Robust distributed spectrum sensing in cognitive radio networks,‖ in Proc. IEEE INFOCOM, 2008.
[14]. K. Zeng, P. Pawelczak, D. Cabric, ―Reputation-based cooperative spectrum sensing with trusted nodes assistance,‖ IEEE Lett. Communication, vol. 14, pp. 226-228, (2010).