ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

# Detection of Malicious Node in Wireless Sensor Network under Byzantine Attack

Jayanti Pandey, Dr. Achala Deshmukh

M.E Student, Department of Electronics & Telecommunication, Sihngad College of Engineering, Pune, India

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

**ABSTRACT:** Wireless sensors network (WSN) is intended to be deployed in environment where sensors can be exposed to circumstances that might interfere with measurement provided. Data fusion is used which overcome sensors failure and coverage problem in mobile access wireless sensor network under Byzantine attacks. In Byzantine attacks, compromised sensors send false sensing data to the gateway leading to increased false alarm rate. Static attack and dynamic attack are two possible attack strategies. However due to high computational complexity of the optimal scheme parameters for q-out-of-m rule, this rule is infeasible as network size increase and/or the attack behaviour changes. First, 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 false alarm rate and miss detection probability will be recorded under static and dynamic attacks.

**KEYWORDS:** Wireless sensor network, Byzantie attacks, Distributed detection

## I. INTRODUCTION

Wireless sensor networks are the combinations of tiny sensors which communicate with each other using wireless communication. Sensor networks provide unique opportunities of interaction between computer systems and their environment. Each sensor node monitors some physical phenomenon (e.g., humidity, temperature, pressure, light) inside the area of deployment. The collected measurements are sent to a base station. The communication range of sensor nodes is limited to tens of meters and hence not all of them can directly communicate with the base station. Therefore, data are sent hop-by-hop from one sensor node to another until they reach the base station. Although a sensor node is capable of sensing, data processing and communication, their limited memory capacity, limited battery power, low bandwidth and low computational power make it vulnerable to many kinds of attacks. The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the traffic flow. There are lots of attacks on these networks which can be classified as routing attacks and data traffic. Some of data attacks in sensor nodes are wormhole, jamming, selective forwarding, sink hole, byzantine attack etc.

A serious threat to wireless sensor networks is the Byzantine attack [1], 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 the packet in order to conserve the resources. In wireless sensor network byzantine attack has following types concerned with nodes: Selfish Attack, Black Hole attack, Wormhole attack, Gray Hole attack. Here we consider 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 fusion centre by transmitting fictitious observations. The rest of the sensors are referred to as honest, and they follow the expected rule of operation. However,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

due to its high computational complexity, the optimal q-out-of-m scheme is infeasible as the network size increases and/or the attack behaviour changes. To overcome this limitation, effective sub-optimal schemes with low computational complexity are highly desired. First, propose a simplified, topology construction which construct and maintains an efficient network topology by using linear q-out-of-m scheme proposed to minimize the false alarm rate and miss detection probability. Second, a detection of malicious node is done using adaptive data fusion under time-varying attacks. If any malicious nodes are detected it reports to the base station and the base station raises the alarm to the end user. The end-user monitors the environmental details and again sends the request to the base station.

**Attacks on Wireless Sensor Networks**

Wireless sensor networks are susceptible to wide range of security attacks due to the multi-hop nature of the transmission medium. Also, wireless sensor networks have an additional vulnerability because nodes are generally deployed in a hostile or unprotected environment. There is also no standard layered architecture of the communication protocol for wireless sensor network.

Table.1 Layering based attacks and possible Security approaches as follows:

| Layer | Attacks | Security Approaches |
|---|---|---|
| Physical Layer | Denial of Service<br>Tampering | Priority Messages<br>Tamper Proofing<br>Hiding, Encryption |
| Data Link Layer | Jamming<br>Collision<br>Traffic manipulation | Use Error Correcting Codes<br>Use spread spectrum techniques |
| Network Layer | Sybil Attack<br>Wormhole Attack<br>Sinkhole, Flooding | Authentication<br>Authorization<br>Identity certificates |
| Transport Layer | Resynchronization<br>Packet injection attack | Packet Authentication |
| Application Layer | Aggregation Based Attacks<br>Attacks on reliability | Cryptographic approach |

## II. BACKGROUND AND RELATED WORK

A realistic approach is to minimize the worst miss detection probability, which guarantees that the misdetection probability will not exceed that advertised the worst case, no matter which distribution is used by the Byzantine sensors. Author in [3] propose a new approach to automated response called the response and recovery engine (RRE).These engines employ a game-theoretic response strategy against adversaries modelled as opponents in a two-player Stackelberg stochastic game. Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, and Minyi Huang, Member, IEEE [4] propose a Mean field Game Theory approach which can be applied to distributed networks having multiple players. The research make the nodes in MANET self reliable in defending the attacks by making strategic decisions depending upon the results obtained from the game theory

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

approach. Xiannuan Liang and Yang Xiao, Senior Member, IEEE [5] have review the existing game-theory based solutions for network security problems, classifying their application scenarios under two categories, attack defence analysis and security measurement. Reliable data fusion in wireless sensor networks with mobile access points (SENMA) is considered under both static and dynamic Byzantine attacks, in which the malicious nodes report false evidence with a fixed or time-varying possibility, respectively. In SENMA, the mobile access point (MA) traverses the network and collects the sensing information from the individual sensor nodes. The adversary has full control over some of the authenticated nodes and can perform arbitrary behaviour to disrupt the system. In distributed detection, due to power and bandwidth constraints, each sensor, instead of sending its raw data, sends quantized data (local decision) to a central observer or Fusion Center (FC). The FC combines these local decisions based on a fusion rule to come up with a global decision. To address the scenario of unknown local sensor performance metrics, it employs the total number of detections (also referred to as the count statistic) as a decision statistic at the FC [8].

## III. PROPOSED WORK

In this paper, we have proposed a clustering algorithms based on energy consideration i.e. hybrid energy- efficient distributed clustering (HEED). HEED is a hierarchical, distributed, clustering scheme. It allows single hop communication within each cluster and allows multi-hop communication between CHs and base station.CH selection depends on residual energy and intra cluster communication cost. Residual energy is used to set the initial set of cluster heads. Intra cluster communication cost is used for deciding to join a cluster or not. This cost value is based on node‘s proximity or node‘s degree to the neighbour. Each sensor node estimates CHprob value for becoming a CH as follows:

$$CH_{prob}=C_{prob} * E_{residual}/E_{max}$$

This probability value should not **be** beyond the threshold value $P_{min}$; $P_{min}$ is inversely proportional to Emax. This algorithm consists of constant number of iterations. Every node goes through this iteration until it finds a CH that it will be the node with least communication cost. At the end of iteration every node doubles the $CH_{prob}$ value. Iteration will be terminated if $CH_{prob}$ value reaches 1.

We further investigate the performance of the proposed approach under both static and dynamic attacking strategies, in which the malicious sensors send false sensing information with a fixed or time-varying probability. It is found that: without detection, the system has the worst performance under the static attack, where the malicious nodes always send false information; when pre-detection is enforced, the false alarm rates are reduced significantly for all attack strategies. However, dynamic attacks take much longer time to be identified compared to static attacks. Simulation results are provided to illustrate the proposed approaches.

## III. SYSTEM MODEL

A. Sensor Detection

When sensor is used to the sensors quantize their sensing result into a single bit. The sensor sends the sensing reports and applies the fusion rule to make the final decision. One popular hard fusion rule used in distributed detection is the q-out-of-m scheme.

B. Byzantine Attacks

Byzantines intend to deteriorate the detection performance of the network by suitably modifying their decisions before transmission to the fusion centre (FC). The Distributed Detection problem in the presence of Byzantines under the assumption that the Byzantines have perfect knowledge of the underlying true hypothesis is studied. Many studies have also presented the optimal attacking distributions for the Byzantines such that the detection error exponent is minimized at the FC. There are different attack strategies that could be adopted by the malicious sensors.

Static attack: In this strategy, the malicious nodes send opposite data with an arbitrary probability Po that is fixed, with 0 < Po “1”.

Dynamic attack: In this strategy, the malicious nodes change Po after each attacking block, which is composed of one or more sensing periods.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

C. Mobile Access point (MA)
The MA traverses the network and collects the sensing information from the individual sensor nodes. The MA uses the binary reports of the sensor nodes to make the final decision on whether the target is present or absent. This distributed detection problem can be modelled using the conventional binary hypothesis test, where the hypothesis H0 represents the absence of the target, and the hypothesis H1 represents the presence of the target.

D. Polling
The end user collects information of the sensing nodes. Polling is used to collect the n no of user sensing information to MA. When MA can analysis to calculate the polling value and fix which trust and which are not trusted node. It is observed that the proposed linear approach can achieve satisfying accuracy with low false alarm rate. However, there are chances of violating the problem constraint. To enforce the miss detection constraint and improve the data fusion accuracy, we further propose to use the linear approximation as the initial point for the optimal exhaustive search algorithm.

E. Cluster Head
There is a Cluster-Head (CH) per each cluster of sensor nodes which it coverts its radio range nodes shown in Fig.1. So, the malicious node detection process does by cluster heads. If any malicious nodes are detected it reports to the base station and the base station raises the alarm to the end-user. The end-user monitors the environmental details and again sends the request to the cluster head.

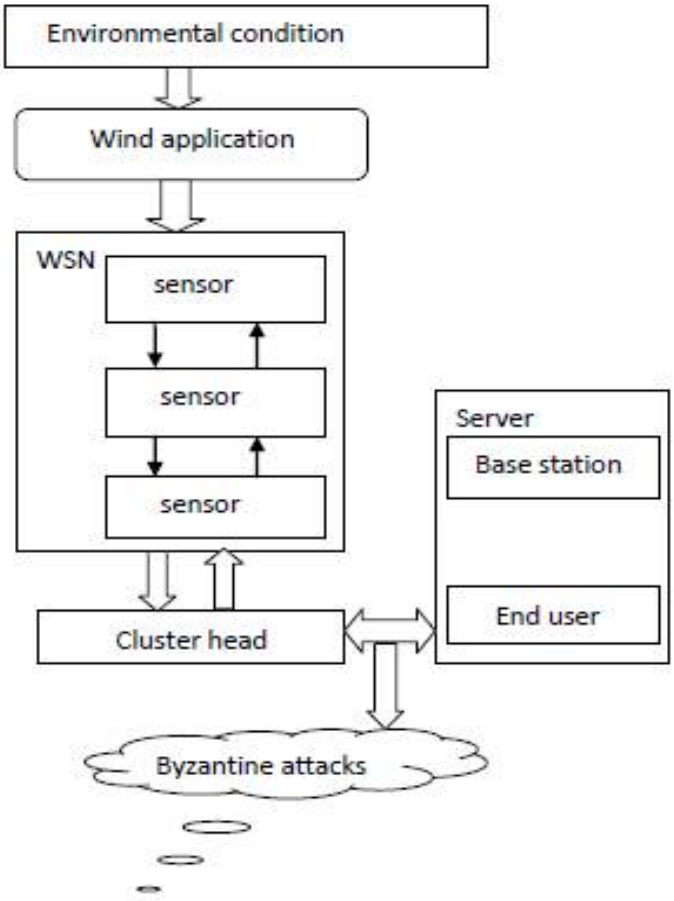


Figure 1 System Architecture [6]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

## IV. SIMULATION RESULT

Intensive simulation experiments using NS2 were conducted to evaluate the effectiveness of our clustering based malicious nodes detection algorithm. In the simulation, the detection algorithm is deployed at a forwarding node to monitor all sensor nodes under the control of the forwarding Node, and the detection is performed every cycle, which is a basic time unit of the simulation. For convenience, the output of sensor node are either as “1” (alarm) or “0” (no alarm). All simulation results were recorded after the system model reached steady state. We assume that a sensor node is compromised randomly by the attacker at a specific probability every cycle, referred to as the attack probability, and then this malicious node keeps reporting the opposite information after compromised. For example, a malicious node always sends “alarm” while the aggregation result computed from other sensor nodes is “no alarm”. Meanwhile, a normal sensor node may also send alarm when real alarm occurs. This case also occurs randomly at a different alarm probability.

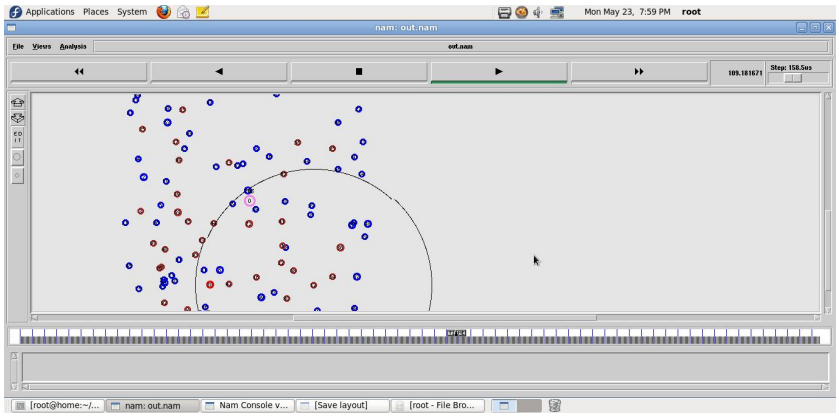


Figure.2. Deployment of network

**Result:**

(a) Throughput

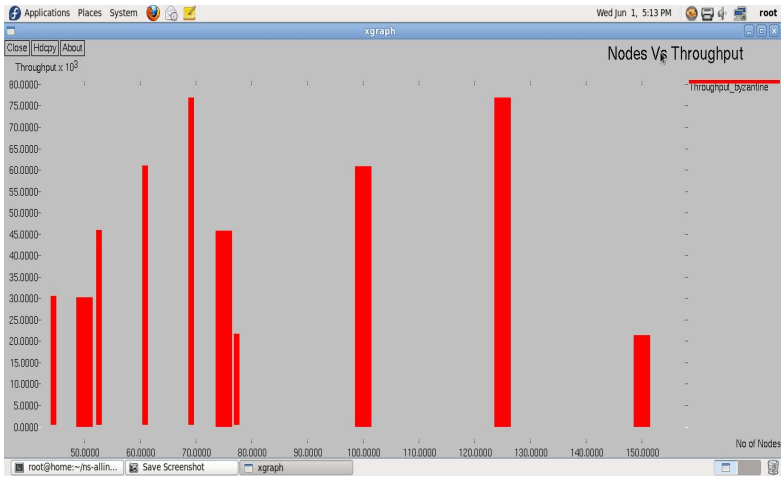


Figure.3 Throughput Comparison

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

(b) Energy Consumption

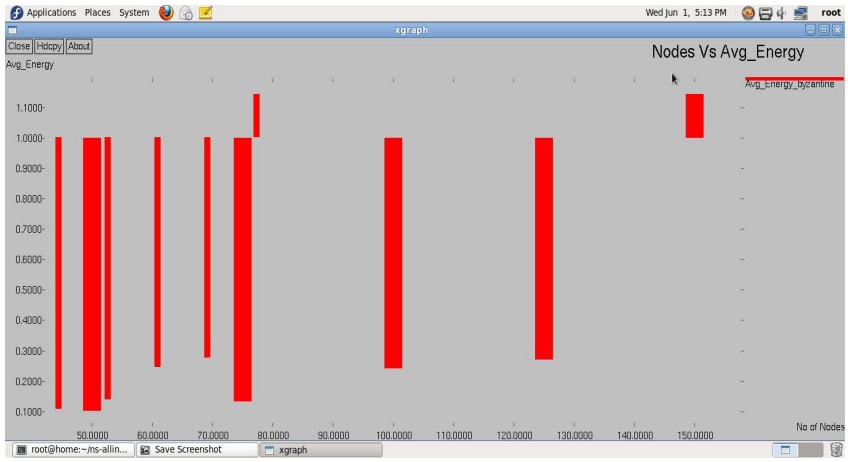


Figure.4 Energy Consumption Comparison

(c) Control Over-heads

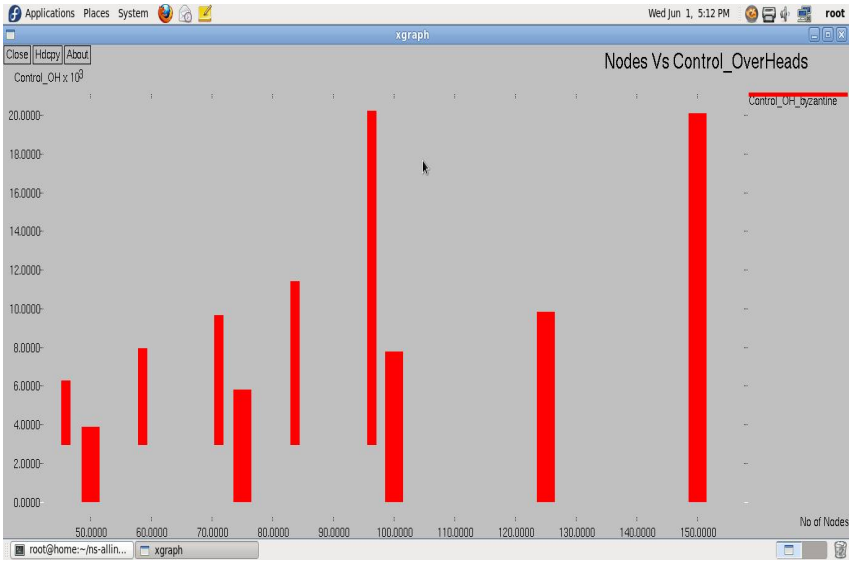


Figure.5 Over-heads Comparison

## V. CONCLUSION

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. We proposed a novel malicious node detection scheme to detect compromised or malicious nodes in wireless sensor networks. 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 Fusion-centres. Analyze the network performance parameter in wireless sensor network. Implementation of nodes in wireless sensor networks using

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

clustering algorithm. We have to detect the alarm at base node. Wireless network technology has been consistently improving with time and increasingly finding its way into all aspects of people's daily lives.

## REFERENCES

[1]. 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.
[2]. 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.
[3]. Saman A. Zonouz, Himanshu Khurana, William H. Sanders, Fellow, IEEE, and Timothy M. Yardley" RRE: A Game-Theoretic Intrusion Response and Recovery Engine" IEEE Transaction On Parallel And Distributed Systems, Vol. 25, NO. 2, February 2014.
[4]. Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang,Senior Member, IEEE, and Minyi Huang, Member, IEEE "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks" IEEE Transactions On Wireless Communications, Vol. 13, No. 3, March 2014.
[5]. Xiannuan Liang and Yang Xiao, Senior Member, IEEE "Game Theory for Network Security" IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, First Quarter 2013.
[6]. M. Abdelhakim, L. Lightfoot, and T. Li, ―Reliable data fusion in wireless sensor networks under Byzantine Attacks, IEEE Military Communications Conference, MILCOM 2011, Nov. 2013.
[7]. 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.
[8]. Bhavya Kailkhura,Swastik Brahma,Yunghsiang S. Han and Pramod K.Varshney, "Optimal Distributed Detection in the Presence of Byzantines" 2013 IEEE.
[9]. Stefano Marano, Vincenzo Matta, and Lang Tong, Distributed Detection in the Presence of Byzantine Attacks" IEEE Transactions on Signal Processing, vol. 57, no. 1, January 2009