INTERNATIONAL JOURNAL OF TECHNOLOGY AND COMPUTING (IJTC)
ISSN-2455-099X,
Volume 2, Issue 3 March 2016.

DETECTING BYZANTINE ATTACK USING WIRELESS SENSOR NETWORK

Shivali Goyal [1], Gurdeep Kaur[2], Dr.Parminder Singh[3]

[1]MTech Student, Shivalig78@gmail.com, Assistant Professor
[2]Assistant Professor, cecm.infotech.gurdeep@gmail.com
[3]Assistant Professor, Singh.parminder06@gmail.com
[1, 2, 3] Department of Information Technology, CEC Landan, Mohali

ABSTRACT

A wireless sensors networks (WSNs) consist of a large number of nodes which spread over a specific area where we want to look after at the changes going on there. In this paper describe the various attacks such as wormhole attack, cloning, sinkhole, Sybil, blackhole and byzantine attack. These types of networks are much vulnerable to security .Much type of active and passive attacks are possible in sensor network. Byzantine attack is the most common and harmful attack. This attack degrades network performance and leads to denial of service attack. The attack is triggered by the malicious node which is present in the network. Novel technique has been proposed to detect and isolate malicious node from the network. The novel technique is based on trust values. It will improve network efficiency in terms of packet loss, delay and increase throughput of the network.NS2 simulator tool will be used in it.

Keywords: *Byzantine attack, AODV Protocol, WSNs, CBR.*

I. INTRODUCTION

Wireless sensor network is a combination of tiny light weight wireless sensors with computing elements.These sensor nodes is generally cheaper in price, with limited energy storage and limited processing capabilities. These type of networks are deployed in hostile environment [1] Wireless sensor network monitor the system or environment by measuring physical parameters such as humidity, pressure and temperature. WSNs are best suited for applications like wildlife monitoring, military command, intelligent communications, mat buildings, examining human heart rates [2].There are two types of sensor nodes in wireless sensor networks, sensor node and a sink node. A large number of sensor nodes are there in wireless sensor a network which collects or sense the data and transmit it to the sink through multiple hops. The sink can use that data locally or globally using internet. Sensor node use battery power as an energy source. Battery is a limited power resource and as wireless sensor networks are usually deployed at hostile environment, so power consumption is major concern in wireless sensor network [3]. If the node is not able to communicate through direct link it means the node is out of coverage area. The data can be sending to the other node by using the nodes in between them. This property is referred as multi-hoping. All sensors nodes

work cooperatively to serve the requests. Generally WSNs are not centralized one as there is peer-to-peer communication between the nodes. So there is no requiring of prior established infrastructure to deploy the network.

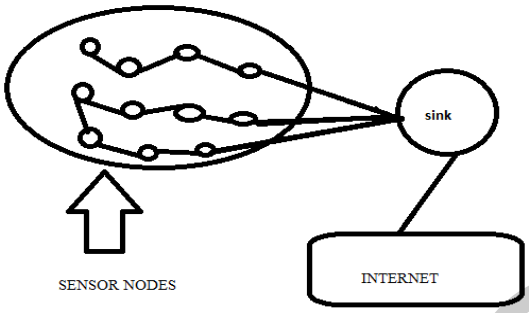

Figure. 1: Wireless Sensor Network [1]

II. Security in wireless sensor networks

Cloning attack: It is the opening point to a large span of insidious attacks such attack, a rival uses the credentials of a compromised node secretly introduces replicas of the node in the network.[4] These replicas are then used to commence variety of attacks that subvert the goal of the sensor application, and the operation of the underlying protocols. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem.

Sinkhole attack: The attacker tries to attract the traffic from a particular region through it when it has some knowledge of routing protocols. For example, the attacker can announce fake optimal path by marketing attractive power, or high quality routes bandwidth to a particular region.

Wormhole attack: In this attack, a malicious node, at one location in the packets to another location in the network tunnels them, to the location where packets are present into the network [5]. When the control messages are disrupted. It is the network layer attack. The two colluding attacker's tunnel between them is referred as wormhole.

Sybil attack: In this attack an attacker makes several illegimate identities in the sensor network either by fabricate or stealing the identities of legitimate nodes [6]. This attack is mostly straightforward to perform in wireless sensors network where the communication medium is broadcast and same frequency is shared among all nodes.

Byzantine attack: In this attack intermediate compromised node carries out the attack such as creating collisions forwarding packets or non optimal paths, routing loops and dropping packets selectively which results in interruption or dreadful conditions of the routing services.

Why byzantine attack:

Reason for choosing the byzantine attack is that not easy for identification as compared to other attacks. Since the network seems to be operating very normally in the view of the user. There is very less research and work on this byzantine attack.

Table 1: Attacks on different layers in wireless sensor network and DOS Defenses

Layer	Attack	Denial-of-service Defense
Transport Layer	Flooding De-synchronization	Client puzzles
Network layer	Routing attacks like black hole,sinkhole,sybil and wormhole	Authorize and monitoring
Data link layer	Collision	Error-correction code
Physical layer	Jamming attack, Tempering	Spread spectrum

III. Literature Survey

Number of work has been done related to our topic. Some important works are described below:

Ju young Kim and Ronnie D. Caytiles (2013) presented a study of the different vulnerabilities, threats and attacks for wireless sensors networks. Effective management of the threats associated with wireless technology requires a sound and through assessment of risk given the environment and development of a plan to mitigate identified threats. An analysis to help network managers understand and asses the various threats associated with the use of wireless technology and a number of available solutions for countering those threats are discussed. Wireless sensors networks provide a numerous opportunities for increasing productivity and minimizing costs. It provides significant advantages for many applications that would not have been possible for the past. The different vulnerabilities threats and attack that could possibly put WSNs in a vital or critical situation have been identified and discussed in this paper. The different categories of these threats are defined to identify a possible countermeasure scheme applicable for each threat classification.

Teodor Grigore LUPU (2012) presented that security has become the forefront of network management and implementation. The challenge in security issues to find a well balanced situation between two of the most important requirements: the need of developing networks in order to sustain the evolving business opportunities and work level, and the need to protect classified, private and in some cases even strategic information. The application of an effective security policy is the most important step that an institution can take to protect its network. Networks have grown in both size and importance in a very short period of time. If the security is compromised, there could be serious consequences

Starting from theft of information, loss of privacy and reaching even bankruptcy of that institution. The type of potential threats to network are continuously evolving and must be at least theoretical known in order to fight them back, as the rise of the wireless network implies that the security solution become seamlessly integrated, more flexible.

Aditya Vempaty (2013) introduced that the control of the false discovery rate (FDR) for distributed detection in wireless sensors network (WSNs) can provide substantial improvement in detection performance over convential design methodologies. In this paper, further investigate system design issues in FDR-based distributed detection. They demonstrate that improved system design may be achieved by employing the Kolmogorov-Smirnov distance metric instead of the deflection coefficient. They also analyze the performance of FDR based distributed detection in the presence of byzantines.Byzantines are the malicious sensors which send the falsified information to the fusion centre(FC) to deteriorate system performance. It is observed that detection performance is degrading when fraction of Byzantines is large. Detection simulation results are providing to demonstrate the robustness of the proposed adaptive algorithm to byzantine attacks in WSNs.

Chris Karlof, David Wagner (2003) considered routing security in wireless sensors networks. Many sensors network routing protocols have been proposed but none of them have been designed with security as a goal. They proposed security goals for routing in sensor networks, show how attack against ad-hoc and peer-to peer networks can be adapted into powerful attacks against the sensors networks, introduce two classes of novel attacks against the sensors network like sinkholes and HELLO floods and, analyze the security of the entire major sensors network routing protocols.

IV. Proposed Solution

In this solution sensors are deployed on the far places to sense the information. The major issue of sensor networks is battery consumption and security. These Proposed Technique clustering is the most efficient type of technique to reduce energy consumption of the sensor node. In this work novel technique is proposed which is responsible to detect and isolate malicious node from the network.

Novel Algorithm:

Start ()
Step 1: *Firstly we deploy the wireless sensor network with fixed number of mobile nodes and in fixed area.*
Step 2: *Divide the whole network into fixed size clusters and select cluster head in each cluster.*
Step 3: *Cluster head selection ()*

a. *Node=0 /// Node identification*
b. *For(i=0;i<n; i++)*
    a. *If(distance and energy (a(i)<a(i+1);*
    b. *Node=a(i);*
    Else
    Node=0;
    End

Step 4: *The shortest path will be established from cluster head to sink.*
Step 5*: Verify secure path ()*

a. *Get coordinate of node whose id is 0*
b. *For(i=0; i<n; i++)*
c. *A(i)=a(i-1)+18;*
d. *End*
e. *Calculate distance between all nodes()*

a. *Distance=(a(i+1)-a(i)^2+(a(y+1)-a(y))^2*

Step 6*: If (any nodes adjacent node! = saved information)*

Step 7*: That node will be detected as malicious node in the network.*

End

V. Experimental Setup

Consider a scenario in which N sensors are deployed. In byzantine attack nodes are senses through wireless sensors network. In this paper number of nodes are 81 which are deployed over area 800*800.Routing protocol Adhoc On- Demand Distance Vector Routing (AODV) is used in this byzantine attack. It is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. In this attack antenna uses omidirectional in nature and MAC layer 802.11 is used. In AODV Route Discovery process begins with the creation of a route request packet and source node creates it [13]. The packet contains source node's IP address, source node's current sequence number, destination IP address, destination sequence number. There are different queues are used in different attacks but in byzantine attack priority queue is used. The traffic type constant bit rate (CBR) is used. This term used in telecommunications, relating to the quality of service. Constant bit rate encoding means that the rate at which a codec's output data should be consumed is constant.CBR is useful for streaming multimedia in network.

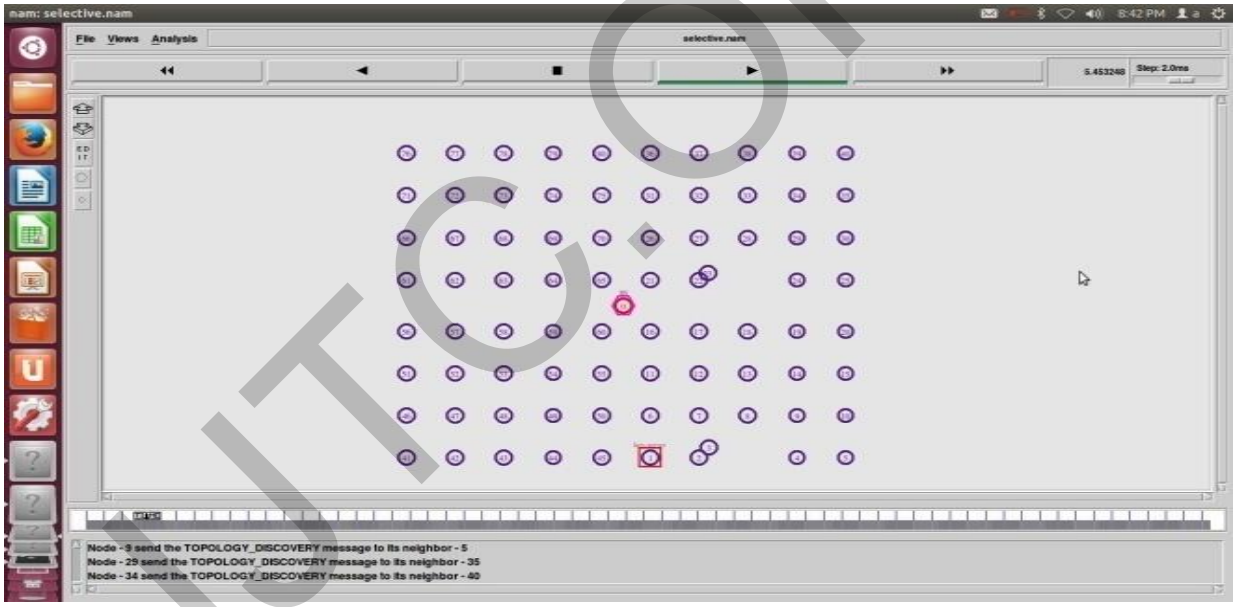

Figure 2. Topology Discovery

VI. Simulation Results

This section represents the simulation results in the support of byzantine attack. We consider WSN model where no of nodes N=81 sensors nodes are deployed in 800*800 square region of interest. When the byzantine sensors are present in the network then they try to manipulate the data and send false information to the base station [14]. There are two graph energy and delay which show how energy are consumed on per node and how the number of packet loss on delay time.

Table 2: Simulation Parameter

PARAMETER	VALUE
Simulator	NS2
Channel Type	Wireless channel
Antenna Model	Omidirectional
Number of mobile nodes	81
Network Interface Type	MAC Layer 802.11
Simulation Time	50 sec
Routing Protocol	AODV
Region area(m)	800*800

Energy Graph

This graph represents the how many energy consumed on per node. It is the ratio between the energy consumed per node to the total number of time. As illustrated in fig 3 due to presence of malicious node in the network which can trigger byzantine attack which leads to increase in energy consumption and after isolation of byzantine attack energy consumption reduced in the network.

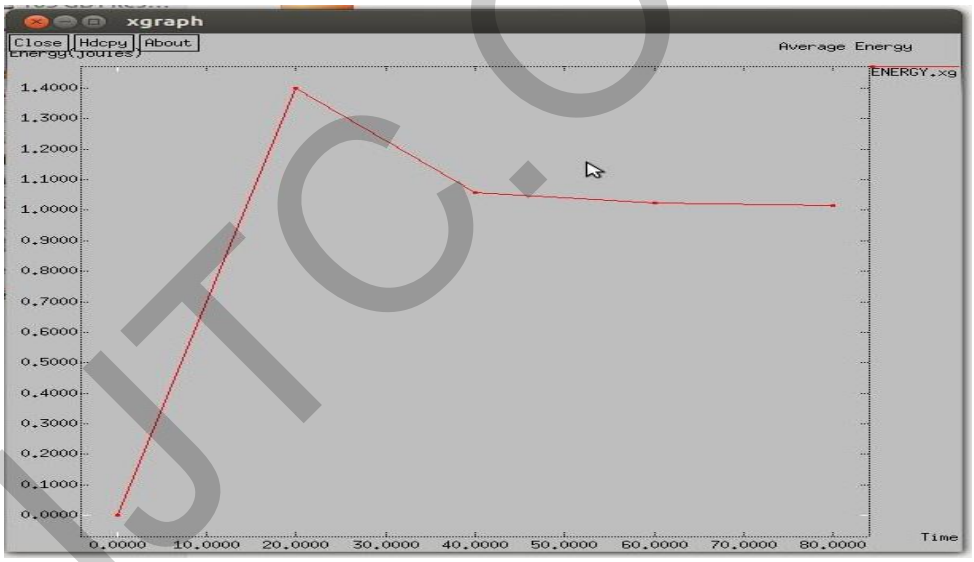

Fig 3. Energy Graph

Packet drop

Packet drop is also known as packet loss ratio. It is the ratio of total dropped packet from source to destination at specific time.

$$\textbf{Packet loss} = no.of\ packet\ send - no.of\ packet\ receive$$

As illustrated in fig 4, the proposed technique will detect and isolate malicious nodes from the network which are responsible to trigger byzantine attack. The graph shows that packet loss reduced when malicious nodes are detected from the network.

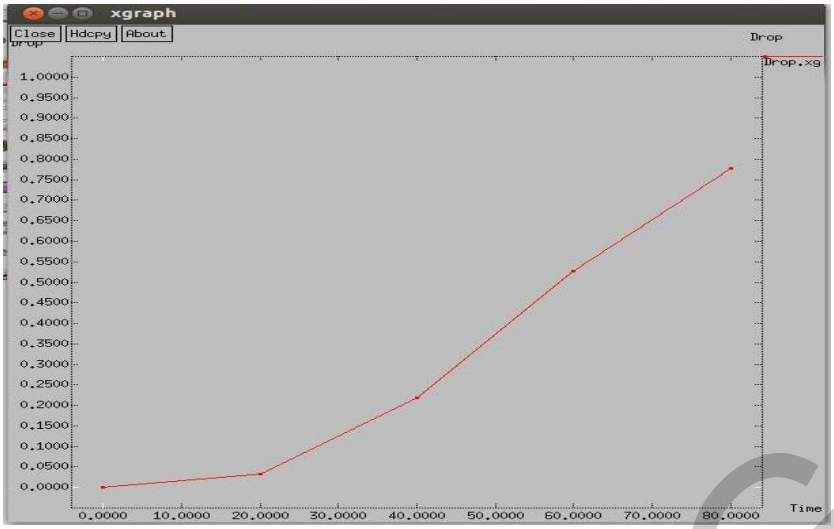

Fig 4. Packet Drop

VI. Conclusion

When the mobile nodes are mutually true, it leads to the reliable data transmission between the mobile nodes. But the main problem occurs during the drop of packet. Drop of packet is due to byzantine attack. To detect and isolate byzantine Attack trust value based scheme has been used. So here low performance of system can be improved by prevent them from internal attacks by detecting packet dropping. Due to packet drop, path is lost easily. This is designed to find out the packet drop nodes and those nodes are then isolated from the path forming a new path for the sending packets to its destination. This work will helps to reduce the problem occur in link failure and packet lost problem. Now the performance degradation problem will also improve.

Acknowledgement

First and foremost I would like to thank Ms Gurdeep Kaur assistance professor, Chandigarh engineering college, landran for her support and encouragement. I also want to thank Dr. Parminder Singh, assistance professor, Chandigarh engineering college, landran for providing valuable advices as my co-guide. They really helped me a lot while writing this paper.

References

[1] Jen-Yeu Chen and Yi-Ying Tseng, "Distributed Intrusion Detection of Byzantine Attacks in Wireless Networks with Random Linear Network Coding", IEEE, 2013 pp. 67-69

[2] Ju Young Kim, Ronnie D Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" Journal of Security Engineering, 2014, pp. 34-37

[3]Teodor Grigore LUPU, "Main Types Of Attack in Wireless Sensors Network", Recent Advances in Signals and System, ISSN: 1790-5109

[4] Amir Shiri et.al "New Active Caching Method to Gurantee Desired Communication Reliability in Wireless Sensor Networks" 2012

[5] Dr. G.Padmavathi,Mrs.D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security,Vol. 4, No.1 & 2,2009,pp.1-9

[6] Kalpana Sharma and M K Ghose, Wireless Sensors Networks: An Overview on its Security Threats"IJCA Special Issue on "Mobile Ad -hoc Networks" MANETs, 2010 pp.42-45

[7] Teodar-Grigopou, Main Types of Attacks in Wireless Sensor and Systems or Network", Recent Advances in Signals and Systems, ISSN: 1790-5109, 2009

[8] Aditya Vempaty, Priyadip Ray, Pramod K.Varshney (2014) proposed in their paper, False Discovery Rate Based of Byzantines", Distrubuted Detection in the presence of Byzantines", IEEE Transactions on Aerospace and Electronic System VOL.50, NO.3 JULY 2014

[9] Samir Athmani, Djallel Eddine Boubiche and Azeddine Bilami, Hierarchical Energy Efficient Intrusion Detection System for Byzantine Attacks in WSNs", IEEE 2013

[10] Vinay Soni, Partik Modi, Vishvash Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network", International Journal of Application Volume 2, Issue 2, February 2013

[11] C.Perkins, E. B. Royer, S. Das,Ad hoc On-Demand Distance Vector(AODV) Routing- Internet Draft",RFC 3561,IETF Network Working Group, July 2003.1

[12] Ahmad Salehi S., M.A. Razzaque,Parisa,Naraei,Ali,Farrokhtala,Detection of sink hole Attack in wireless sensor networks,"IEEE International Conference on Space Science and Communication(Icon Space),1-3July2013,Melaka,Malaysia,pp.361-365

[13] Wang Chun-Hsin and Li Yang-Tang, "Active Black Holes Detection in Ad-Hoc Wireless Networks", Ubiquitos and Future Networks (ICUFN) 2013 Fifth International Conference on Da Nang, pp.94-99, IEEE, 2013

[14] Ju young Kim, Ronnie D.Caytiles, Kyung Jung Kim, A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks,"Journal of Security Engineering, 2014

[15] Baviskar B.R, Patil V.n, "Black hole Attacks mitigation and prevention in wireless sensor network", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp.167-169, May 2014.