International Journal of Latest Trends in Engineering and Technology
Vol.(7)Issue(3), pp. 470-478
DOI: http://dx.doi.org/10.21172/1.73.562
e-ISSN:2278-621X

SECURITY PROTECTION ACROSS NETWORK BASED ATTACKS IN MESH NETWORKS

SUKHPREET KAUR SAINI[1], DR.PARMINDER SINGH[2] AND GURDEEP KAUR[3]

Abstract- This paper commences the secure communication model for wireless mesh networks. There are bulk numbers of Mesh nodes in Wireless Mesh Networks which collect information and transfuse it to Base Station among common hops. In this presented paper the types of attack will be discussed and the solution to overcome these attacks will be examined. A denial of service (DoS) or distributed denial of service (DDoS) attack is the most vital attack and these attacks will be taken up. This malicious node in this attack hits on the accessibility of a node and all nodes in the whole of the network. Purpose of this attack is to block the services of the Mesh nodes. The attacker generally uses battery exhaustion method and radio signal jamming. Denial of Service attacks is transported by outside nodes which break the communication channel among communicating sensor nodes. In DDoS attack, the attack is performed by more than one machine. The proposed approach tracks the sequence number of packets. If packet sequence number is missing then generate the alarm. This alarm makes alert to every node present on the network.

Keywords: Denial of Service (DoS), mesh nodes, Base station, Distributed Denial of Service (DDoS), threshold.

I. INTRODUCTION

Mobile Wireless Networks is one of the very significant technologies to dominate the world of wireless networking for years to come. They furnish adaptive and flexible network connectivity to network nodes anywhere and anytime. Mobile networks, while rendering variety of benefits also bring forth some staggeringly inevitable and vulnerable security issues because of their very features. The nodes in WMNs might have distinct resources available (e.g. hardware) and undergo distinguishable security requirements. The ability of WMNs to provide multiple types of network services and the presence of distinct resources in these networks raise the importance of having different levels of security services. There are two types of wireless nodes in Wireless Mesh networks, Mesh node and a Base Station node. A large number of Mesh nodes are there in Wireless Mesh Networks which collects or sense the data and transmit it to the Base Station through multiple hops. The Base Station can use that data locally or globally using internet.

[1] *Chandigarh Engineering College Landran-Kharar Highway, Sector 112 Landran, Mohali, Punjab, India*
[2] *Chandigarh Engineering College Landran-Kharar Highway, Sector 112 Landran, Mohali, Punjab, India*
[3] *Chandigarh Engineering College Landran-Kharar Highway, Sector 112 Landran, Mohali, Punjab, India*

1.1 Mesh Architecture

The traffic in Wireless Mesh Network depends on number of queries generated per Mean time. The Base Station node transmits the information to be sensed by sending a query throughout the Mesh field. The Mesh nodes respond to the query by gathering the data using their Mesh’s. Ultimately when the Mesh nodes have the result of the injected query will reply to the Base Station node through some routing protocol. A Mesh node also aggregates the replies to a single response which saves the number of packets to send back to the Base Station node [4].

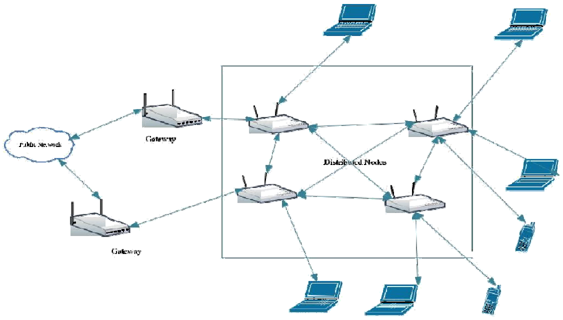

Fig 1: Wireless Mesh Architecture

Table 1: Major Roles of Architecture in OSI Layer

Major Layer	**Roles**
Network Layer	Mesh router, Gateway
Data Link Layer	Data transfer used in this layer
Physical Layer	Radio (RF) Communication

1.2 Security Threats

1. Confidentiality

Information confidentiality is maintained, using encryption with the pair-wise link keys LKMN (symmetric) in exchange messages. Only the two communicating parties can read the exchanged information. Regular and on- demand renewal of these link keys is performed to protect the network from compromised nodes.

2. Integrity

A common method of message authentication code (MAC) is used with each message to guarantee message integrity. Keyed-Hash Message Authentication Code (HMAC or KHMAC) is used. Any change made by the adversary can be detected at next-hop node or at the receiver's end (single-hop destination). Multi-route delivery mechanism is proposed to ensure message delivery and to detect the altered message or the possible malicious node in the route.

3. Authenticity

Each node authenticates other corresponding node wrap on the hash chain element it receives from the sender node in each message. The current message received from a particular sender is authenticated by taking hash of the hash-element associated with that message and then comparing it with the previous message from the same source.

1.3 Attacks in WMN

These attacks are as follow:

1. Worm hole Attack: In wormhole attack, a malicious node, stores packets at a point location in the network and tunnels them to another location. When the control messages are routing are tunnelled it create breakage. It is a network layer attack. The solution of this problem is monitoring the network and flexible routing schemes.

2. Byzantine Attack: In this attack, a moderate compromised node carries out attacks such as creating collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or bad conditions of the routing services. When the byzantine attack occur in the WMN, the performance of WMN starting to decrease. Some performance metrics such as packet delivery ratio, end to end delay and packet loss, also occurred.

3. Denial of Service Attack (DoS) or distributed denial of service (DDoS): A denial of service (DoS) or distributed denial of service (DDoS) attack affects the availability of the network services or simply partitions the network. It decreases a network's ability to perform accurately according to its anticipated capacity in a timely manner.

Table 2: DoS vs. DDoS Attacks

Parameter's	**DoS**	**DDoS**
Attack Perform	Centralized, local only	Distributed
Target	Only single server	Attack on Thousands of machines
Complexity	Low	High
Identification	Moderate	Hard to detect
Impact	Infect 10 to 20 Machines	Infect on the whole network

II. RELATED WORK

Miralem Mehic, Jiri Slachta, MiroslavVoznak, "Whispering through DDoS attack", Perspectives in Science, 2016**,** to contemplate the mechanism in the machines that are involved in the attack. The hidden information will not be able to process by the victim if his computing capacity is less than that of data volume. There should exist a machine that can control the data throughput to increase the flow of converted communication.

Omar Cheikhrouhou, "Secure Group Communication in Wireless Sensor Networks: A survey", Journal of Network and Computer Applications, 2016**,** presents the study of components that are group key management and group membership management of the dissimilar SGC schemes in which there performance and efficiency are discussed.

Jen-Yeu Chen and Yi-Ying Tseng (2013) introduced in their paper, "Distributed Intrusion Detection of Byzantine Attacks in Wireless Networks with Random Linear Network Coding**"**, suggested the locating algorithm to apply RLNC for locating Byzantine nodes in the network. The algorithm can find the areas where some normal nodes and adversary nodes are situated and sometime the normal nodes are mistakenly consider as adversary nodes. To remove the chances of mistakes, the shift scheme is used.

III. PROBLEM STATEMENT

In DDoS (routing disruption attack) the main aims to defect the routing scheme which leads to the unavailability of its network services. Examples of DoS attacks at different protocol layers are channel jamming, wormhole attack, Sybil attack, black hole, and grey hole attacks. In this paper we will apply the proposed model that provide the degree of trust on the network. The result is to mark the value of that node which is suspicious. The behavior of a node can be changed over time. Therefore, node A, can decide about E's behavior as bad, good, or excellent with the help of the experienced degree of trust. The grading of a node to be called as good or bad can be adjusted by the network designer according to the environmental conditions of the ~~n~~etwork.

$$\frac{a}{b} = \sum_{i=1}^{n} \binom{n}{d} x^{-k}$$

From above equation,
1 to n: is the number of nodes to verify the malicious node in the sensor area.
d : is the distance assigned to n nodes.
–k : is the worst case if the malicious node identified.

Suppose in fig no.2, the malicious node k as identified as malicious node if the threshold value is less than 50. In fig 2, the communication between two nodes is node 2 and node 5, but unknown node can get the information from the link (2, 5).

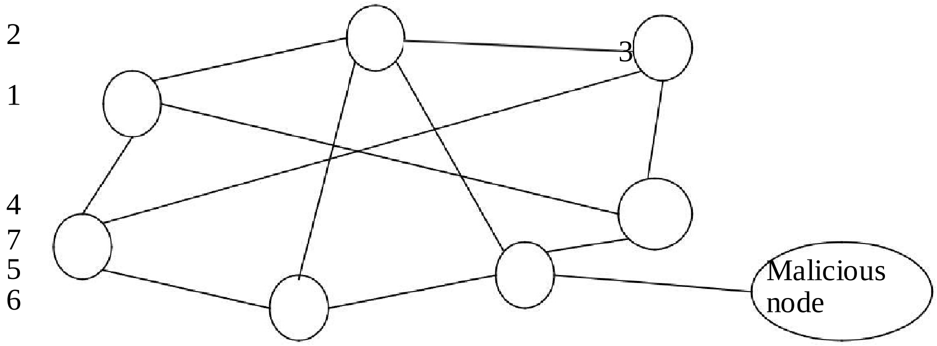

Fig 2: Ipv4 Packet Access

Incoming Packet

Base Station

Determine Route

Update information

Route Selection

If
threshold
<50

Yes

Identify sequence number of the packet

No

Send the packet

Route termination

No
sequence number is missing

If

Resend the packet

Yes
Invalid route

Shutdown the connection

Fig 3: Proposed Flowchart

The possibility of the attack can be reduced if we are using the proposed technique as mentioned in fig 3. This flow chart shows the technique to minimize the attack. Incoming packets pass through network and after that the route is determined. After fixing the route, selection of route is done. If threshold is less than 50 then the packet sequence number is identified, after this the missing number is identified if any sequence number is missing then the route is invalid and the connection is shut down and if there is no missing sequence number the packet is sent to the route termination . If the threshold is more than 50 then the packet is send to the route termination. At last the information is updated to the base station.

IV. EXPERIMENTAL SETUP

Network with 6 to 25 are taken, each with different speed between 1 and 10 meters per second. The pause time values describe the movement of the objects. Each of the objects can move at a random direction, stop for some time (per the pause time), and then change its direction at random and move again. The traffic pattern models the voice data transferred from one node to the other. The data is sent at a rate of 2 kbps to represent compressed voice data.

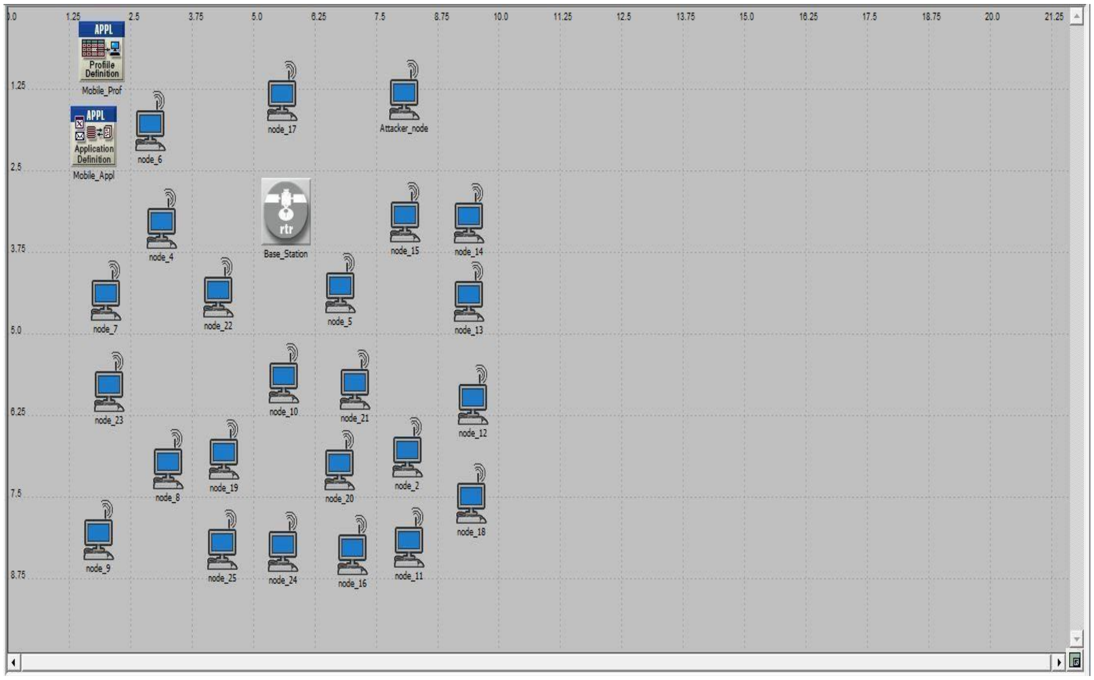

Fig 4: DoS Attack in OPNET

V. RESULTS

5.1 DoS Attack

The following results have been analyzed in this report.

5.1.1 Load

Load increase when the DoS attack is performed on the network and this increased in load will affect the performance of whole network. Increase in load every time will also make congestion in network. In present case load is analyzed at base station because base station is important part of every single node that analyze the traffic that is why the load of base station and wireless LAN are equal. That is why analysis is done that how the black hole acts in the network scenario.

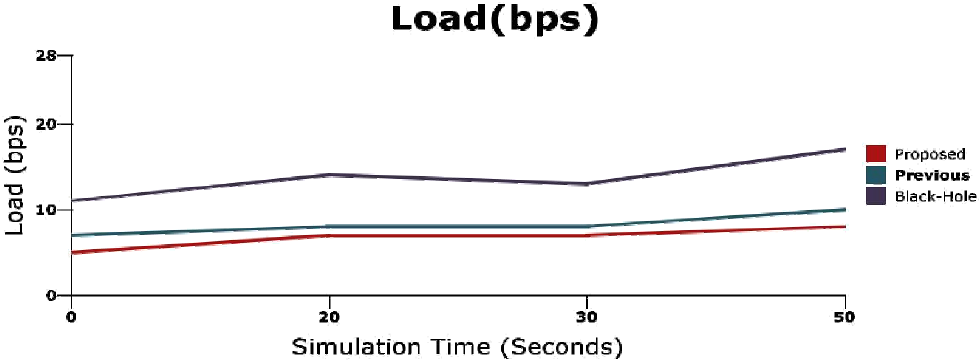

Fig 5: Load in Base Station

5.2.2 Throughput

The meaning of throughput is that number of sends packet is equally to the packet received by the destination machine. In case of black Hole situation increasing in load can affect the throughput and packets that are not received by the destination router properly.

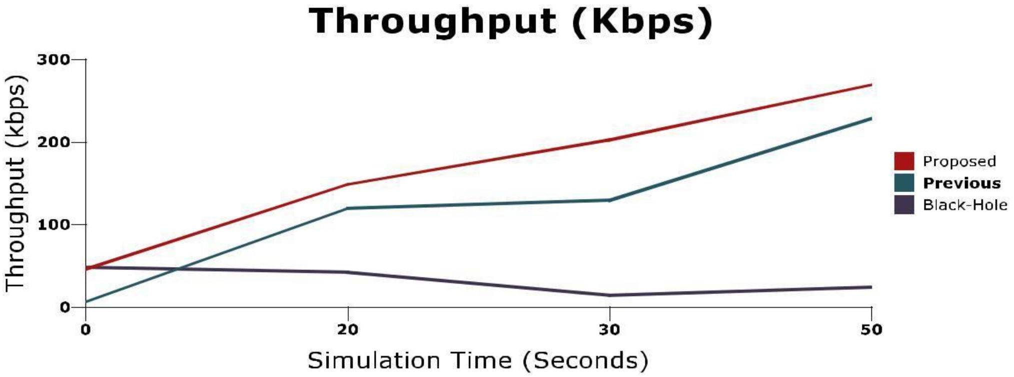

Fig 6: Throughput

VI. CONCLUTIONAND FUTURE WORK

Denial of Service Attack is implemented in this in this paper. Network attack models are assumed that exploit the weakness of the present network. By collecting the evaluation metrics from the attacking scenarios, the impacts of attack upon the existing network are then studied. More research is needed in the mobility of the nodes in order to comprehensively evaluate the impact of the malicious nodes' movement on the protocol's performance.

Table 3: Throughput

Parameter	Previous	Proposed	Black-Hole Attack
Minimum	48	48	24
Average	120	140	42
Maximum	228	269	48

Table 4: Load

Parameter	Previous	Proposed	Black-Hole Attack
Minimum	7	5	10
Average	8	6	11
Maximum	9	7	12

REFERENCES

[1] MiralemMehic, Jiri Slachta, MiroslavVoznak, "Whispering through DDoS attack", Perspectives in Science, 2016,pp.1-6.

[2]Omar Cheikhrouhou, "Secure Group Communication in Wireless Sensor Networks: A survey", Journal of Network and Computer Applications, 2016,pp. 115-132.

[3]Teodor Sommestad Fredrik Sandstrom, "An empirical test of the accuracy of an attack graph analysis tool", Information & Computer Security, Vol. 23, Iss 5,2015 pp. 516 - 531.

[4]Haithem Al-Mefleh, Osameh Al-Kofahi, “Taking advantage of jamming in wireless networks: A survey” Computer Networks, 2016,pp.99-124.

[5]Vincenzo Gulisanoa, Mar Callau Zoria, Zhang Fua, Ricardo Jimenez-Perisb, Marina Papatriantafiloua, Marta Patino Martinez, “STONE: A streaming DDoS defence framework”, Expert Systems With Applications, 2015,pp. 9620-9633.

[6]Ravneet Kaur, Sarbjeet Singh, “A survey of data mining and social network analysis based anomaly detection techniques”, Egyptian Informatics Journal,2015,pp.1-6.

[7]Alan Saied, Richard E .Overill, Tomasz Radzik, “Detection of known and unknown DDoS attacks using Artificial Neural Networks”, Neurocomputing,2016,pp.385-393.

[8] Wolfgang John Tomas olovsson, “Detection of malicious traffic on back-bone links via packet header analysis”, Campus-Wide Information Systems, Vol. 25, issue 5,2008, pp. 342 - 358.

[9]Satish Vadlamani, Burak Eksioglu, Hugh Medal, Apurba Nandi, “Jamming attacks on wireless networks: A taxonomic survey” ,2016,pp. 76-94.

[10]Boping Duan, Jing Liu, Mingxing Zhou, Liangliang Ma, “A comparative analysis of network robustness against different link attacks” , Physica A,2016,pp. 144-153.

[11] Parminder Singh, “Comparative study between unicast and multicast routing protocols in different data rates using vanet”, Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014,pp. 278-284.

[12] Harjot Bawa, Parminder Singh, Rakesh Kumar, “An efficient novel key management scheme for enhancing user authentication in a WSN”, International Journal of Computer Network and Information Security, 2013.

[13] Parminder Singh, “Design an Framework of Wireless Sensor Networks by Preventing Malicious Nodes Attack”, International Conference Elsevier, 2014,pp.195-200.