EXPERIMENTAL EVALUATION TO MITIGATE BYZANTINE ATTACK IN WIRELESS MESH NETWORKS

[1]Sunil Kumar, [2]Er.Vinod Kumar Sharma

Abstract-**The wireless mesh networks consist of number of number that is connected to each other for sharing the information only. The information flow from one to another node through link, channel or could be a path. The sharing of information from one user to another only when the network was authenticates. The information could not be share on unauthorized network. The authorized network is a network that connects two machines each other and also identifies to each other, then the three-way handshake connection built on both side and mutually exchanges the packet. This paper explaining the concept of Byzantine attack which was more powerful attack studied in the previous papers. This attack creates virtual connection on both side then after intercepts all the information from two node just say node u and node v. This paper explores the prevention technique by using Pre-shared key technique. The proposed pre-shared key technique implemented on the network simulator-2 software and evaluated the performance parameters viz. throughput, packet delivery ratio and end to end delay.**

*Keywords:***Throughput, malicious node, Delay, byzantine, mesh network, access point.**

I INTRODUCTION

The Ad-Hoc network is a peer to peer network that connects number of wireless nodes that directly communicate with each other. The wireless Ad-Hoc network is infrastructure less network and used in civilian applications, home automation etc. The mesh topology used in this paper and focus is to deploying the Ad-Hoc network in such a way that forward and transfer the data from one node to another node. The wireless mesh based network creates an Ad-Hoc network and each random node transfer the data or payload to another in the same Ad-Hoc networks. The Ad-Hoc network also communicates [12] with the wired network as below in the figure 1. The node 0 establishes the wired connection between two nodes i.e. node 5 and node 6 where the rest of all nodes connected in a wireless manner. Here the node 0 communicates with IEEE 802.3 standard whereas the IEEE 802.11 makes wireless connection to all 6 nodes.

The remainder of the paper is organized as follows: the next section provides the background of classification of attacks, the byzantine attack follows and had same signatures of wormhole attack and section research challenges explained the challenges faces to prevent this byzantine attack. Then the previous research efforts that contribute to our approach are reviewed and an described in section: Related work.

 All Rights Reserved © 2014 IJSETR

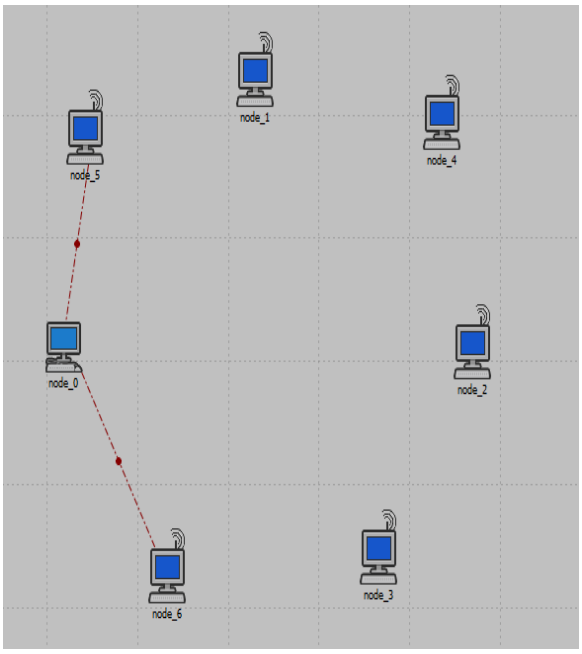

Fig1: Wired- Wireless Network Scenario

The section IV is explaining the working of proposed scenario and different result analyzes from the section V. The concluded work of this paper are mentioning on the end of section before references.

A. Attack Classification

The attack can be classified into two ways: Internal Attack and External Attack. The external attack carried out by the external node to the authenticated network and forwards false information to gain useful information. This attack generally wrap the own ip address to the authenticate node ip address and the internal nodes compromised with the nodes. The congestion related problems and unavailability of services rises in this type of attack [9].

The internal attack fully compromised with the internal node that communicates with neighboring nodes. The malicious node compromised with the internal nodes and gain information to every information flow in the network. This attack has more harmful than external attacks. The unavailability of service, connection termination, packet losses problems arises in this type of attack. This paper explored the byzantine attack, therefore we highlights some of internal attacks described below in this section:

II. RESEARCH CHALLENGES

Wormhole attacks are difficult to detect since the maliciousnodes only eavesdrop and retransmit the beacons [2]. Theattacker creates a low-latency link (i.e. high-bandwidthtunnel) between two or more attackers in the network.Attackers promote these tunnels as high-quality routes tothe base station[1]. The following attack classification [1] shown in the table 1.1.

Table 1.1: Attack Classifications [1]

Layers	**Attack**
Physical layer	Tampering, Eavesdropping, Jamming
Link/MAC-layer	Collision, Exhaustion, Unfairness, IdentitySpoofing, Traffic manipulation
Network/routing layer	Spoofing, False routing, Packet replaying,Selective forwarding, Neglect and greed,Homing, Misdirection Blackhole, Grayhole,Byzantine, Wormhole, Sinkhole
Transport layer	De-synchronization/ Forwarding, ClockSkewing, Data aggregation, Distortion,Selective message, Flooding

III. RELATED WORK

Majid Meghdadiet.al. (2011), explained the wormhole attack generally used by the attackers. The attackers created two low latency points on the network and then add the sensor node, these nodes act as malicious nodes that access the information of the different nodes. A malicious sensor node that can communicate with all other sensor nodes within its range poses a thread to the functional efficiency of the data collected in the network called ‘internal attack’. The paper explained the sinkhole attack, this attack targets a specific source node, and it may affect the availability of the victim node. In a sinkhole attack, the intruder usually attracts the network traffic by advertising itself as having the shortest path to the base station. Packet-relay-based

 All Rights Reserved © 2014 IJSETR

wormhole attacks can be launched by one or more malicious nodes. A malicious node relays data packets of two distant sensor nodes to convince them that they are neighbors.

Weichao Wang, Aidong Lu (2007), proposed an automatic detection algorithm with appropriate user interactions to handle complicated scenarios that include a large number of moving nodes and multiple wormhole attackers. This paper explored the development of approaches that can detect attacks on wireless networks directly based on their impacts on the network topology. The proposed approach will use the measurement results to build the distance matrix among the wireless nodes and reconstruct the network topology using incremental Multi-dimensional scaling (MDS). A normalized wormhole indicator value will be calculated for every node to identify those suspicious areas' under wormhole attack

Ismail Hababeh et.al. (2010), described that Wormhole attack distorts the network topology and decrease the network systems performance. They worked on Ad Hoc network and described the risks of wormhole attacks. The wormhole attack could be divided into three categories, namely, hardware attacks, broken protocol wormhole attack and malicious protocol. In hardware based attacks, the attacker can use out-of-band channel, or use higher transmitting power to make a wormhole in network. In broken protocol based wormhole attacks, the malicious nodes don't follow the requirements of specific protocols during data transmission. In the malicious protocol attacks, the adversary may use its own protocol to change the data packets during transmitting. The most typical wormhole attack of this type is encapsulation where a nasty node is located somewhere in the network and heard a routing request. Generally, normal wormhole attack, the adversary attempts to convince other network nodes that there exists a path between two locations, but in fact there is no path between the nodes.

Steve Glass et.al. (2008), WMN is distinct from manets in that it uses multiple radios and relies on a high-speed back-haul network. A secure MAC layer is responsible for ensuring that a mesh network carries traffic only for authorized stations, thus preventing attacks by unauthorized ones. Two keys used to prevent the attacks like Preshared key (PSK) and Public key (certificate-based). Pre-shared key (PSK) approaches use passphrases or other key material provided to each station in advance. Public key (certificate-based) approaches use private keys to authenticate each station's identity. This paper suggested that Public-key-based approaches are extremely flexible and use certificates to verify station identities.

IV. PROPOSED SCENARIO

The proposed scenario is depicted in Fig. 2. The source node transmitsbroadcast UDP traffic. This ensures that its packets aretransmitted back-to-back and that the source node does not waitfor any ACK messages. The used routing mechanism is a byzantine node that transmitsthe messages on the local active nodes as assumed in the practical layout. We have measured a maximum link bandwidth of about 1 MB/s. This bandwidthcan be achieved in both directions of a link almost independently of the data transfer inthe other direction.

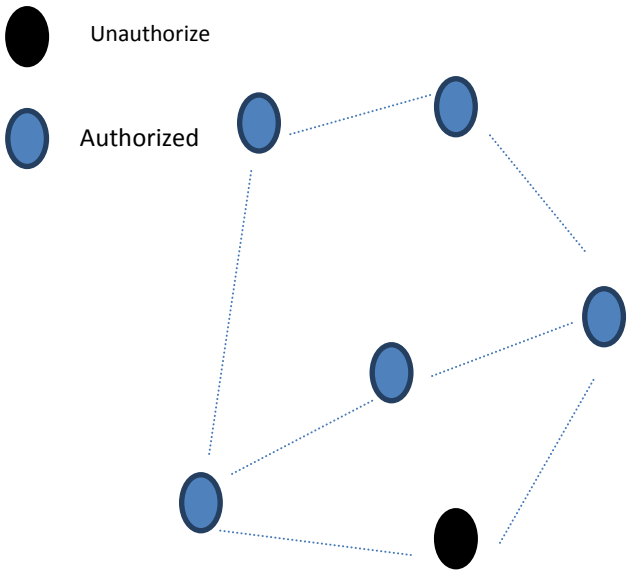

Fig2. Proposed Scenario

V. RESULT DISCUSSION

I. Delay: Rises of delay de-accelerates the performances of the networks. In the Byzantine attack the delay depends on the packet delivery ratio if the delivery ratio is slow that means delay absolutely increases that why the performance of the network degrades, because more number of packets falls on the network. In the figure 4, the byzantine attack discovered by the proposed scenario by electing leader node and shared the key among

 All Rights Reserved © 2014 IJSETR

communicating nodes. The delay decreases that mean the packet delivery ratio increases and more the number of packet transfers from any destination and that acknowledge the same source node.

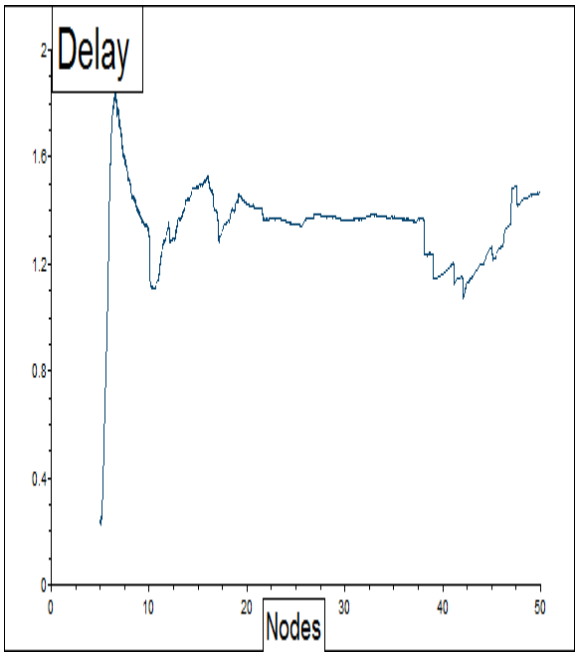

Fig3: Delay of Byzantine Attack

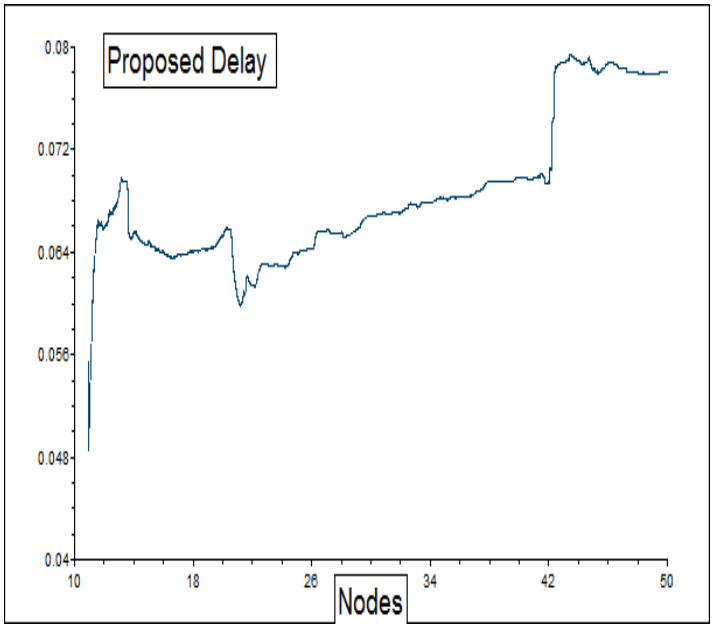

Fig4: Proposed Delay

II. Throughput: The Throughput calculates the total number of packets sent to the source machine and receives by the destination machine. When byzantine occur then it degrades the overall performance of the network because more the number of packets dropped by the malicious node whereas the proposed work prevented the byzantine attack resultant achievable throughput are high then byzantine attack.

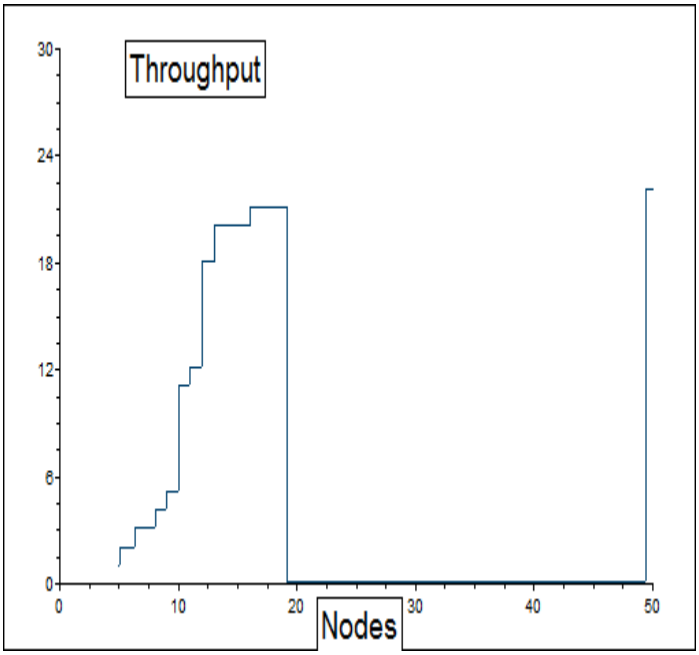

Fig5: Throughput of Byzantine Attack

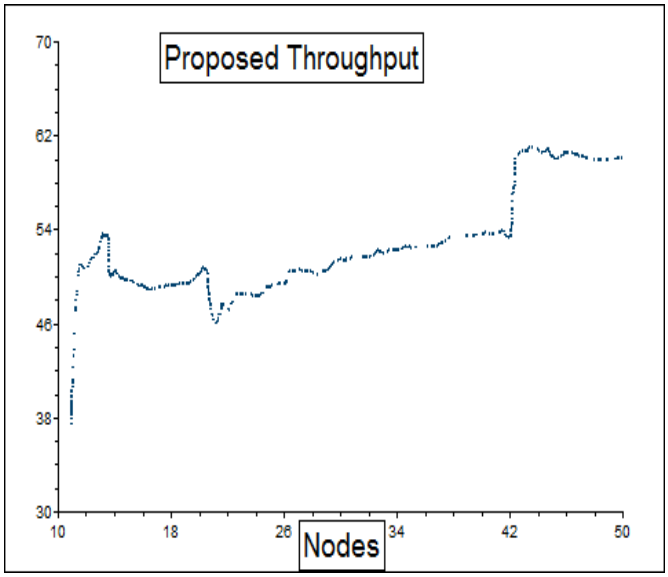

Fig6: Proposed Throughput

 All Rights Reserved © 2014 IJSETR

VI. CONCLUSION

We have analyzed from this paper that byzantine attack breaches the security and access useful information from the wireless networks. The wireless network was any Ad-hoc network that attach to wireless nodes and handset. The IEEE 802.11 MAC based standard imported on the scenario, we add malicious node on the authenticate network that access the information. When the malicious node access the information via virtual connection then it forms 'Byzantine Attack". This paper presents the prevention method that implemented on the scenario and remove wireless vulnerabilities, security threats in the mesh based topology. The Pre-shared key technique was applying on the nodes that avoid such type of these vulnerabilities. We analyzed that when this technique by applying on the scenario, therefore it improves the throughput and minimizes the delay of the wireless mesh networks.

REFERENCES

[1] Majid Meghdadi, SuatOzdemir,InanGuler,"A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE technical review, 2011, pp.89-102.

[2] Weichao Wang, Aidong Lu, "Interactive wormhole detection and evaluation",Information Visualization,2007,pp.3-17.

[3]IsmailHababeh,IssaKhalil,AbdallahKhreishah,SamirBataineh, "Performance Evaluation of Wormhole Security Approaches For Ad-Hoc Networks", Journal of Computer Science,2013,pp.1626-1637.

[4]Ping Yi, Yue Wu, Futai Zou, Ning Liu, "A Survey on Security in Wireless Mesh Networks",IETETechnicalReview,2010,pp.6-14.

[5]Om Shree, Francis J. Ogwu, "A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks", SciRes. 2013,pp.76-83.

[6]SteveGlass,MariusPortmann,VallipuramMuthukkumarasamy,"Securing Wireless Mesh Networks",IEEE,2008,pp.30-36.

[7] www.ns2.org

[8]Noureddinekettaf,hafidabouaissa,pascallorenz,"An efficient heterogeneous key management approach for secure multicast communications in ad hoc networks, Telecommunsyst, 2008,pp.29-36.

[9] Umesh Kumar Singh, ShivlalMewada, Lokeshladdhani, Kamal Bunkar, "An Overview and Study of Security Issues &Challenges in Mobile Ad-hoc Networks (MANET)", IJCSIS, 2011,pp.106-111.

[10] www.opnet.com

[11] Parminder Singh, "Comparative study between Unicast and Multicast Routing Protocols in Different Data Rates Using VANET.", In: International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014,pp. 278–284.

 All Rights Reserved © 2014 IJSETR