BYZANTINE ATTACK ON WIRELESS MESH NETWORKS: A SURVEY

Sunil Goyal[1]
M.Tech Student, Deptt. of CSE
GKU TalwandiSabo ,India

Vinod sharma[2]
Assistant Professor, Deptt. of CSE
GKU TalwandiSabo ,India

Abstract-The wireless mesh networks connected to the different network but it routed the data properly from one direction to another direction. Each node progressively sends data to another through access points; the individual nodes are also share the data to one another. From the communication perspective point of view, when any unauthorized node enter on the authorized network could access the information without any notification. The byzantine attack treated like wormhole attack where the attacker node (or malicious node) scumble the local or wide area networks.

Keywords: malicious node, layer-2, layer-3, byzantine, mesh network, access point.

1. INTRODUCTION

The wireless mesh networks is the extension of the Ad-Hoc wireless networks that exchanges the data on number of nodes that is connected with the mesh type topology. WMNs consist of a wireless backbone with mesh routers. The wireless backbone provides large coverage, connectivity, and robustness in the wireless domain [10]. Ad hoc networks provide routing using the end-user devices, the network topology and connectivity depend on the movement of users [10]. These end user devices also share information to each other; the end user nodes also communicate to other node which is located on the other side of the network also. The fig.1 states the internetwork access points that connected to each other and formed extended service set (ESS); the ESS authenticate itself that is why they share the information to each other. The information broadcast by the access point itself and this information heard by the other access point that is authenticated and convey to the other nodes.

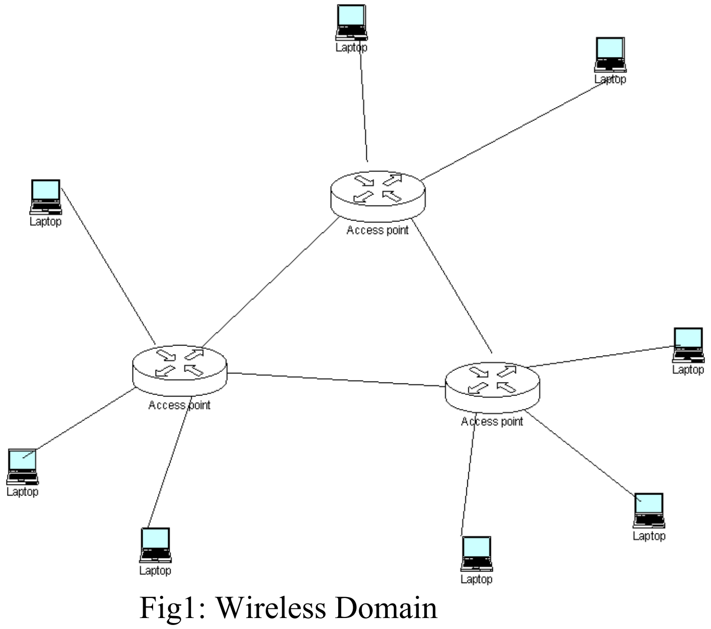

Fig1: Wireless Domain

The fig.2 represents the mesh based wireless topology that connected to the number of other nodes and these nodes treated as a peer to peer, the information unicast transmitted to the other node of the same network.

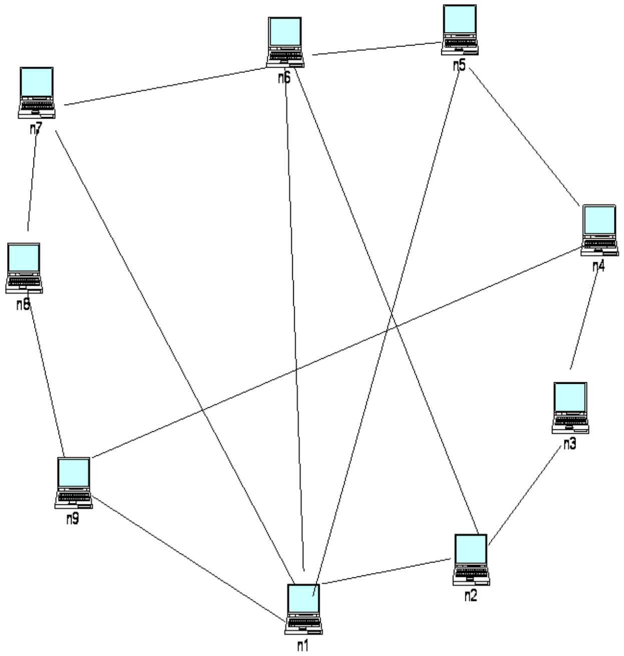

Fig2: Wireless mesh nodes

2. CLASSIFICATION OF ATTACKS

If the mesh based topology is best among other topology but there are some cons of the network. The major problem of any network is security; because any attack performed on the network based topology. The attack breaches any security of the network; attack harmful for any authorized and authenticates networks. There are number attacks since 1990s and some famous attacks generally formulated below [5]:

Table 1: OSI Layer Attacks

OSI Layers	Attacks
Routing Layer	Blackhole, Greyhole, Byzantine ,Sybil ,Cache Poisoning, Message Bombing
MAC Layer	Unfairness , Selfish , MAC Misbehavior

The routing layer attack performed on the layer-3 of the open source interconnection (OSI) model, this type of provide fake packet information by the malicious node, the malicious node is an unauthorized node that access the information of any communicated node of the network. It can also change the complete routing information structure of the Ad-Hoc network.

The MAC is a medium access control layer that works on the Layer-2 of the open source interconnection (OSI) model, the malicious node enter on any network or make any machine's fake MAC address that compromised with other node of the network and affect the overall network performance.

2.1 BYZANTINE ATTACK

The Byzantine attack is the more powerful attack (act like wormhole attack) from the open source interconnection (OSI) model as shown in table 1. The malicious node that compromised the authenticate node and creates a virtual connection between the authenticate nodes as shown in fig.3.

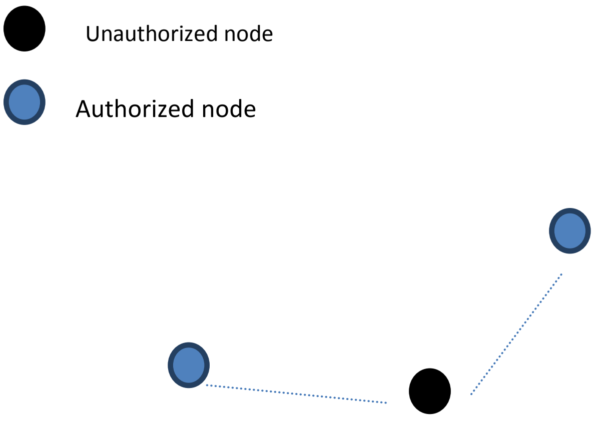

Fig.3: Byzantine Attack

These maliciousnodes exhibit Byzantine behaviour and can manipulate routing metric to influence route selection decisions. We mainly focus on wormhole attacks launched by malicious nodes, since route discovery is carried out by malicious nodes on behalf of mesh clients [1]. Byzantine wormhole attacks using neighbourhood connectivity information [1]. When node forward packet, the nodes watchdog verifies that the next node in the path also forward the packet. Watchdog does this by listening promiscuously to next nodes transmissions. If next node does not forwards the packet, then it is misbehaving node. Path rater uses this knowledge of misbehaving nodes to choose the network path that is most reliable to deliver packets [8].

3. LITERATURE SURVEY

Akyildiz Ian f., wangxudong, kiyon (2005), had emerged as a key technology for next-generation wireless networking. Because of their advantages over other wireless networks, WMNs are undergoing rapid progress and inspiring numerous applications. The Authors aim to provide a better understanding of research challenges of this emerging technology. WMNs will be integrated with the Internet and many other wireless networks, and thus transport protocols for WMNs need to be compatible with TCPs. Although WMNs can be built up based on existing technologies, field trials and experiments with existing WMNs prove that the performance of WMNs is still far below expectations. The Authors explained throughout the article, there still remain many research problems. Among them, the most important and urgent ones are the scalability and the security.

SomanathTripathy(2013),proposed that how ADOV routing protocol cures the Byzentine attack. He presents two possible solutions. The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. Computer simulation shows that compared to the original ad hoc on-demand distance vector (AODV) routing scheme.

YairAmir,BrianCoan,(2011),proposed that Performance Analysis of MANET under Black hole Attack. They investigated the effects of Black hole attacks on the network performance and simulated Black hole attacks in Qualnet Simulator and measured the packet loss in the network with and without a black hole.

G.S.Mamatha,Dr.S.C.Sharma(2010)presented the adaptive approach to detect black hole and grey hole attack in adhocnetworks. They generated a Path based detection algorithm where each node not necessary watch all nodes, but it only observe the next node in current path. In this ,they analysis the false positive probability taking constant threshold and dynamic threshold. They analysis the great impact of performance under different grey magnitude values.

4. APPLICATION SCENARIO

AODV's routing discovery process allows the middle node send RREP to the source node, in order to reply the RREQ received [4]. When a malicious node in network receives RREQ, it can forge a RREP, claim it has a latest and shortest route to destination node. If this malicious RREP reaches the source node before the correct RREP, which are sent by the real destination node or an intermediate nodes who have a real route to destination node, the source node will mistake that it finds a route to reach the destination node, and sends application layer data to thedestination node along the corresponding opposite direction route of the malicious RREP [4].

5. MONITORING AND ISSUES

Security in terms of authentication and authorization is the main issue for communicating nodes in the local and wide area networks. The number of attack that is not stops by the unicast and multicast protocol [9]. These protocols monitor and maintain the routing protocols when mesh nodes exchange the payload between them. When any unauthenticated data comes on the range of authorized network and that node comprised and behave like authorized node then virtual connection created between the nodes. The following fig. pictured the unauthenticated entered on the authorized networks.

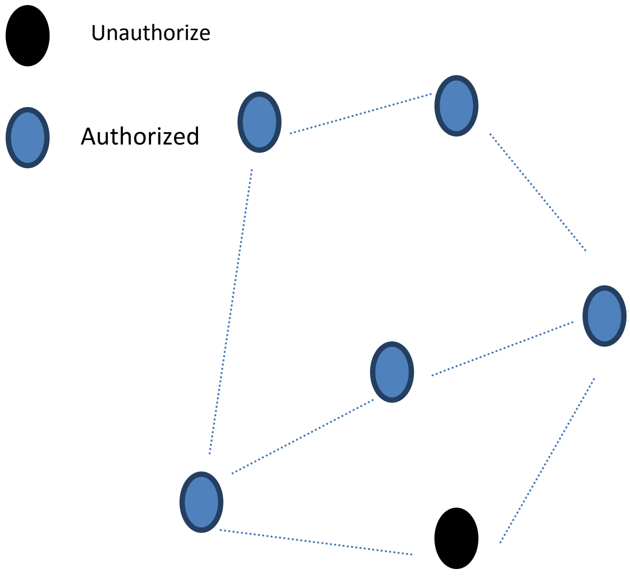

Fig4. Virtual connection established in unauthorized node

6. CONCLUSION

We show number of attacks on the open system interconnection (OSI) model. There number of attack that performed on Layer-2 and Layer-3 of the OSI model. The attacker node (or malicious nodes) that access the information from any authorized network whether it shows identity in local or wide network. The Byzantine attack is the more harmful attack that access the information through the tunnel, therefore we formulate some prevention steps to stops these attacks. These prevention steps will be the future work from this survey paper.

REFERENCES

[1] RakeshMatam and SomanathTripathy, "WRSR: wormhole-resistant secure routing for wireless mesh networks", Springer,2013,pp.1-12.

[2] YairAmir,BrianCoan, Jonathan Kirsch,JohnLane,"Prime: Byzantine Replication under Attack",IEEE,2011,pp.564-577.

[3] YairAmir,ClaudiuDanilov, “Danny Dolev,et.al.,"Steward: Scaling Byzantine Fault-Tolerant

Replication to Wide Area Networks",IEEE, 2010, pp.80-93.

[4] SongbaiLu,LongxuanLi,et.al.,"SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack",IEEE,2009,pp.421-425.

[5] G.S. Mamatha,Dr. S.C. Sharma,"Network Layer Attacks and Defense Mechanisms in MANETS- A Survey",IJCA,2010,pp.12-17.

[6] CharikleiaZouridaki · Brian L. Mark · MarekHejmo, “Byzantine robust trust establishment for mobile ad hoc networks”, springer, 2007, pp.189-207.

[7] zeljkoIlic, AlenBazant,BorivojModlic, “An efficient data rate maximization algorithm for OFDM based wireless networks” , wireless networks, 2010, pp.17-25.

[8] Parminder Singh, DamandeepKaur, “An Approach to Improve the Performance of WSN during Wormhole Attack using Promiscuous Mode”, IJCA, 2013, pp. 26-29.

[9] Parminder Singh, “Comparative study between unicast and Multicast Routing Protocols in different data rates using VANET”, IEEE, 2014, pp.278-284.

[10] Ian F. Akyildiz ,Xudong Wang , Weilin Wang, “Wireless mesh networks: a survey”, computer networks, 2005,pp.445-487.