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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Two Step Technique for Isolation of DDOS Attack in Wireless Mesh Networks

Shubhpreet Rana [1], Aditi Kumar [2]

P.G. Student, Department of Computer Science Engineering, Baddi University of Emerging Sciences and Technology Baddi, India [1]

Associate Professor, Department of Computer Science Engineering, Baddi University of Emerging Sciences and Technology Baddi, India[2]

ABSTRACT The wireless mesh network is the decentralized type of network in which mobile nodes can change its location any time. Due to decentralized nature of the network various type of active and passive type of attacks are possible in the network. The DDOS is the distributed denial of service type of attack in which malicious node flood the victim node. The performance of the network gets reduced in terms of various parameters. In this paper, novel technique is been proposed which detect malicious nodes from the network which are responsible to trigger DDOS attack in the network.

KEYWORDS DDOS, Mesh, Decentralized nature, malicious

I. INTRODUCTION

Wireless network is a term refers to any kind of networking that does not necessitate cable. It is a proficiency that helps telecommunications networks to save costs of cables for networking in specific establishment in their installation. The communication system is usually managed and implemented via radio waves where the implementation takes place at physical level. The nodes connected with the internet through the access point in the wireless network [1]. Wireless Mesh Network is a topology where each node must not only pass around its own data, but also serves as a transmitter for other nodes so it must collaborate to spread the data in the network. A mesh network can be established for a flooding technique or a routing technique. When routing technique is used the messages allocate beside a path, by hopping from node to node until the message reached to the destination. A mesh network using self healing algorithm to guarantee all its paths accessibility, a routing network must allow for continuous connections around broken or blocked paths. WMN is a network made up of radio nodes implemented in a mesh topology. A wireless mesh network is a special type of wireless ad hoc network. A WMN is implemented to provide dynamic and cost effective connectivity over a specified geographical area. On the other hand, in the ad hoc network the wireless devices formed ad hoc when the devices come into communication range of each other. WMN consists of mesh clients, mesh routers and gateways [2]. The mesh clients are laptops, cell phones and other wireless devices and the mesh routers forward traffic to and from the gateways (mesh network). A mesh network is reliable and redundant. By using routing protocol the reliability increased and fast in the speed whenever a packet to be transmitted from source to destination via number of nodes and the many routing protocol has been proposed for wireless mesh network. The routing requirements of any routing protocols are scalability, reliability, performance enhancement, throughput, load balancing, congestion control and efficiency. Routing protocols have number of matrices to calculate the best path from source to destination for routing the packets. The metrics contain a model for measurements that can be how many hops, the routing algorithm used to determine the optimal path from source to its destination for a packet routing. The procedure to find the path is that, the routing algorithms initialize and maintain routing tables, which hold the total routing information for the packets [3]. This routing information is varied from one routing algorithm to another routing algorithm. Routing table

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

has a variety of information which is generated by the different routing algorithm. Mesh Routing protocols have categorized as Proactive, Reactive and Hybrid Routing Protocol. Security attacks in wireless mesh networks depend upon the various factors. It totally depends upon the nature and behavior of the protocol. It is also based on the method of the attacker to use to accomplish their motive, is on impersonation, fabrication, modification, Denial of Service (DoS) and other attacks.

a. Security attack at the Physical Layer of WMNs: An attacker may destroy the external hardware and simply routers are installed at the external area. These routers are sensitive and easily information can be stolen by the attacker. Jamming attack comes under this category [4].

b. Security attack at the MAC layer of WMNs: There are further different types of attacks that can be triggered at Mac Layer.

i. Passive Eavesdropping: The Nature of the WMNs is broadcasting the transmission; it is possible for attacker to launch the passive eaves dropping within the transmission range of the communication nodes. It can be launched in internal as well as external nodes.

ii. Flooding Attack: An attacker sends many MAC control messages to its neighbor nodes. Due to this, the fairness of the medium is physically abused.

iii. MAC Spoofing: An attacker tries to change the MAC address during transmission of frames [5].

c. Security Attacks at Network Layer of WMNs: Main attacks which come under these categories are:

i. Black-hole attack: In black hole attack, the zero metric value is advertised by attacker for all the destination nodes around it to route packet belongs to it. A Malicious node generate the false data-information and forward it, claiming that it has best path and generate second best node to forward packet through malicious node.

ii. Wormhole attacks: In wormhole attack attacker gets packet at one location of network and then access them to another location in network, return result back from that location [6]. When there is tunnel between to clouding protocols is called wormhole attack.

iii. Replay attack: In replay attack, the essential or correct data is transmitted continuously by attacker to inject the network routing traffic that has been used previously by the users.

d. DDOS Attack (Distributed Denial of Services) : A DDoS attack can be defined as an attack which uses a large no. of computers to launch a coordinated dos attack against a single machine or multiple victim machines. A DDoS attack is composed of several elements like attackers, victim, zombies and reflectors.

II. LITERATURE REVIEW

Gassara [2015] explained Wireless Mesh Networks has many security issues. Denial of Service (DoS) among all the attacks represents a huge umbrella of powerful attacks. By identifying the problem of the attacker, attack can be identified. In this paper, they discussed novel approach of IP trace back based on marking approach and Chinese remainder theorem can be used to conceive the communication protocol in WMN IEEE 802.11s environments. At the end they evaluated the performance and the efficiency of the proposed scheme based on some collected evaluation metrics [7].

Szott [2014] explained amendment for wireless mesh networks which is a legitimate network participant hopes to increase its QoS at the expense of others. In this paper they have discussed various attacks and analyze their affects on the network by analyze their performance. Furthermore they explained possible countermeasures and detection methods and attempt to quantify the threat of the attacks to determine which of the 802.11s vulnerabilities need to be secured with the highest priority [8].

Jingle & Raj singh [2014] discussed that wireless mesh networks are highly vulnerable to Distributed Denial-of-Service attacks and having self-configuring property. In this paper they propose ColShield, an effective and collaborative protection shield which not only detects flooding attacks but also prevents the flooding attacks through clever spoof detection. The evaluation of ColShield is done using extensive simulations and is proved to be effective in terms of false positive ratio, packet delivery ratio, and communication overhead and attack detection time [9].

Jiang [2013] proposed a new scheme using the flow trust values to defend against DoS attack. Different from previous schemes, it employs the flow trust to safeguard legitimate flows. A router monitors network flows and calculate flow

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

trust values which are used for queue management. It can be extended to combine with other flows detection algorithms to defend against more DoS attacks [10].

Sachdeva & Singla [2013] explained that WMN is considered as a promising solution for offering self-configuring capabilities, self-healing, low-cost access in broadband services. In this review paper, they reviewed, challenges, security issues and attacks at physical layer, network layers and medium access control wireless mesh backbone and access control in Wireless Mesh Network. In the wireless mesh network, there are number of an issue which affects the performance and efficiency [11].

Sanam, Seetha & Kuriakose [2012] explained that WMN has no central controller. It provides application in various fields of research like local, personal and metropolitan areas. In this paper they have discussed various threats of security and their consequences on the network. They discussed various techniques for detection of wireless mesh network. First of all they introduced DSLR protocol for isolating and preventing DOS attack from the network. Secondly they discussed channel aware detection algorithm which can be used for mitigate selective forward attack which is also a type of Denial of service attack [12].

III. RESEARCH METHODOLOGY

The DDOS is the distributed denial of service attack in which malicious node choose the legitimate node which will trigger attack on the victim node. In the DDOS attack the malicious node will send the control packets to the legitimate nodes and legitimate nodes will send the rouge data packets to the victim node to trigger attack. In the work, technique will be proposed which will detect malicious nodes from the network and to detect malicious nodes following are the steps which are followed:-

1. In the first step, the network is deployed with the finite number of nodes. The fixed bandwidth is allocated to each node in the network
2. The central node start analyzing the bandwidth consumption of each vehicle node and node which is using the bandwidth above allocated value will be the malicious nodes.
3. In the third step, the central node checks the type of packets which the node is sending, which is using the bandwidth above the allocated value. When the node is sending the data packets to the victim node, it may be the malicious node.
4. In the last step, the nodes which is sending the rouge data packets, if that node will receive control packets from any node then that node will be detected as the malicious node which is responsible to trigger DDOS attack .

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

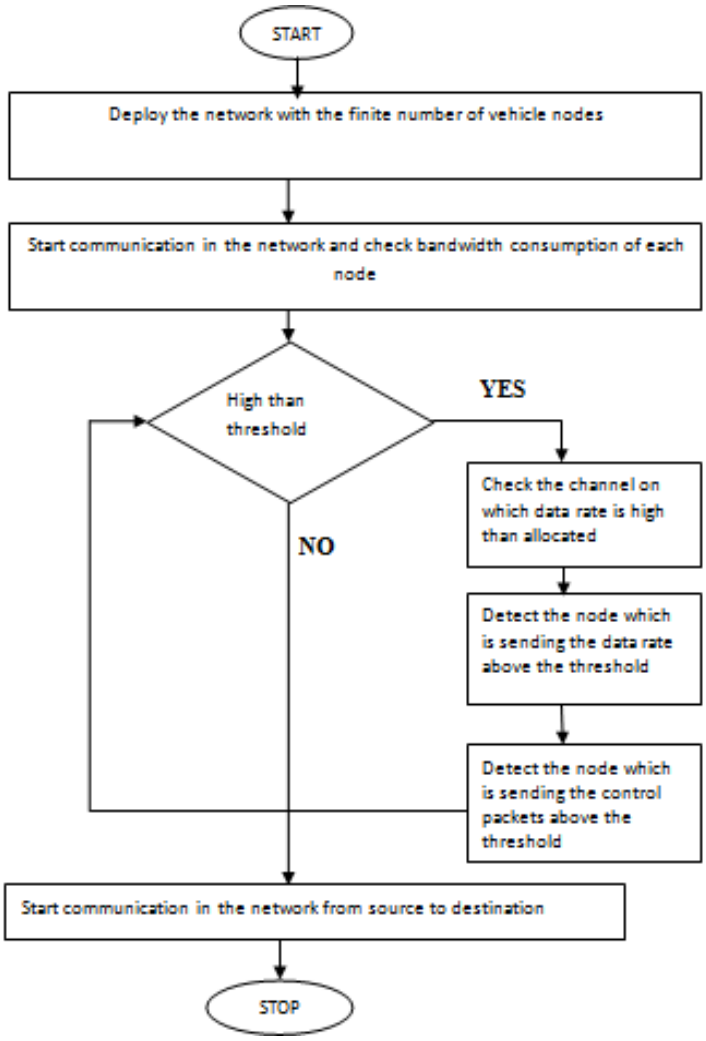

Fig 1: PROPOSED TECHNIQUE

Proposed Algorithm

Input : Number of nodes
Output : Detection of malicious
1. Assign bandwidth the data rate to each node in the network
2. The source node start sending data to destination node
3. if (bandwidth consumption >threshold)
4. Check channel on which data rate is high than threshold
5. Check the node which is sending data packets on the node
6. If (node ==detected)
7. check the node which is sending control packets
8. isolate detected node
9. else
10. no malicious node
11. end

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

12. end

IV. RESULT AND DISCUSSION

The proposed Algorithm is been implemented in NS2 and the performance is analyzed in terms of various parameters which described graphically

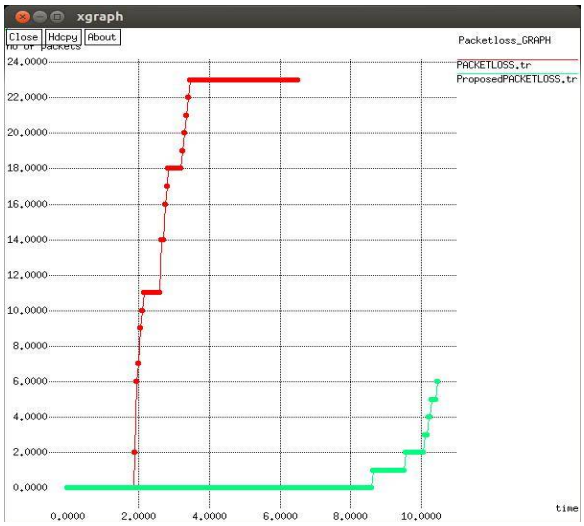

Fig 2: Packet-loss comparison

As shown in figure 2, The packetloss of proposed and existing algorithm is compared and it is been analyzed that packetloss in proposed algorithm is less as compared to existing algorithm

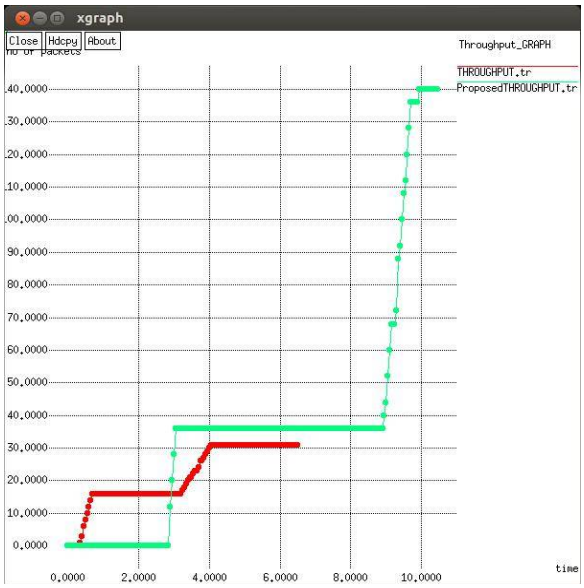

Fig 3: Throughput comparison

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

As shown in figure 3, The throughput of the proposed, existing is analyzed and it is been analyzed that network throughput of proposed technique is maximum due to isolation of DDOS attack

V. CONCLUSION

In this work, it is been concluded that DDOS attack is an active type of attack in which malicious node flood the victim node with the rough data packets. The malicious node joins the network because the mesh network has decentralized nature. In this work, threshold based technique is proposed in which the node, which is sending data above the assigned value (by sending rough data packets) will be marked as malicious. The node which is sending the control packets above the assigned value will be detected as malicious node and will be isolated from the network. The proposed technique performs well in terms of various parameters.

REFERENCES

[1] A. Morais and A. Cavalli, "Detection of Attacks in Wireless Mesh Networks," Dependable Computing (LADC), 2011 5th Latin-American Symposium on, Sao Jose dos Campos, pp. 45-54, 2011.
[2] A. Vlavianos, L. Law, I. Broustis, S. Krishnamurthy, and M. Faloutsos, "Assessing link quality in ieee 802.11 wireless networks: Which is the right metric?" in Personal, Indoor and Mobile Radio Communications, 2008. PIMRC, IEEE 19th International Symposium on, pp. 1–6 Sep. 2008.
[3] W. T. Tan, P. Hu, and M. Portmann, "Experimental evaluation of measurement-based sinr interference models," IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), vol. 4, issue 12, pp. 143-223,2012.
[4] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," Proceedings of the sixteenth annual international conference on Mobile computing and networking, ser. MobiCom, New York, NY, USA: ACM, 1–12, 2010.
[5] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," Dependable and Secure Computing, IEEE Transactions on, vol. 9, no. 1, pp. 101–114, 2012.
[6] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?" Proceedings of the fourth ACM conference on Wireless network security, Elsevier, WiSec, New York, NY, USA: ACM, 2011, pp. 47–52, 2011.
[7] Mouna GASSARA, Imen, Faouzi ZARAI, Obaidat "All-in-One Binary Word Solution for IP Traceback in Wireless Mesh Network", IEEE ICC, - Ad-hoc and Sensor Networking Symposium, volume 10, issue 5, pp. 89-103, 2015,
[8] Szymon Szott, "Selfish Insider Attacks in IEEE 802.11s Wireless Mesh Networks", IEEE Communications, Magazine, volume 4, issue 7, pp. 539-639, 2014.
[9] Diana Jeba Jingle1and Elijah Blessing Rajsingh, "ColShield: an effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks", IEEE, volume 8, issue 13, pp. 18-54, 2014.
[10] Jiang, Shi-wen CHEN, Jiang-xing WU, Xiao-long YE, Tong GUO, "Distributed Denial of Service Attacks Detection Method Based on Conditional Random Fields", Journal of Networks, Vol 8, No 4, 858-865, 2013.
[11] Ratika Sachdeva and Aashima Singla, "Survey on Privacy Issues and Security Attacks in Wireless Mesh Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, 2013.
[12] Ms. Sanam E Anto, Ms. S Seetha and Robin K Kuriakose, "A Survey on DoS Attacks and Detection Schemes in Wireless Mesh Networks", Elsevier, International Conference on Modeling Optimization and Computing (ICMOC), vol 7, issue 2, pp.- 28-35, 2012.