An Intrusion Detection System Against UDP Flood Attack and Ping of Death Attack (DDOS) in MANET

Ankur Ashok Acharya [#1], Arpitha K.M [*2], Santhosh Kumar B.J [#3]
[1,2,3] Department of Computer Science
[1,2,3] Amrita Vishwa Vidyapeetham University
[1,2,3] Mysuru Campus, Karnataka, India
[1] ankuracharya20@gmail.com
[2] arpithamadappa17@gmail.com
[3] santhoshbj50@gmail.com

Abstract **- DDoS is one of the serious attacks in the ad hoc network. Among lot many DDoS attacks, UDP flood attack and Ping of death attack are considered to be important as these two attacks may cause severe damage to the network. To provide better security to the network, efficient intrusion detection (IDS) system is required to monitor the network continuously, keeping track of malicious activities and policy violations and produce report to the network administrator. UDP flood attack and ping of death attack are given importance in this paper as they are not well addressed in the existing research works. Packet capture and packet decoder is used to identify the packets and retrieve the packet details. A threshold is set for each node that is connected to the network. If the packet flow into the node exceeds the threshold that is set then the administrator is notified about the same.**

Keyword - MANET- mobile ad-hoc network, DDoS-distributed denial of service, Intrusion detection system, UDP flood attack, Ping of death attack.

I. INTRODUCTION

Mobile ad-hoc network is a technology that is emerging. It is a group of wireless nodes which is able to communicate without the help of any centralized node; each node is capable of routing packets to this node. A node in MANET moves freely and it can configure itself. It is vulnerable to many kinds of attack due to its mobility and self-routing capability. Nodes in the MANET can even change its link to other devices very often. So, one of the major challenges in MANET today is security, because there is no central controller which exists [1, 2]. Nodes in the MANET assume that all the nodes in the network will help in healthy routing of the packets. This assumption gives the attacker an opportunity to perform DDoS attack on the network [3].

DDoS is one of the main attacks in MANET. DoS attacks do not wish to modify data or gain illegal access, but instead they will crash the servers and the networks, disrupting legitimate users' communication [4]. DDoS is a type of Denial of Service attack where multiple nodes called zombies are used to attack the victim node [5]. Zombies are the vulnerable nodes which are used to initiate the attack. These nodes are installed with attack tools to allow the attacker to perform DDoS attack on the victim node [6].

There are two types of victims.

(i) Primary victims are those nodes which are under attack.

(ii) Secondary victims are those nodes which launch the attack[7].

The incoming packets that flood the victim node may originate from different sources, which may be numerous [8]. Since the sources are many, it is very difficult to know the legitimate user when the attack occurs. There are many types of DDoS attacks: they are wormhole attack, blackhole attack, UDP flood attack, ping of death attack etc [9].

In this research work that is taken up, two specific attacks are being concentrated on; the UDP flood attack and Ping of Death attack. UDP Flood attack, user datagram protocol is a session less networking protocol. In this type of attack, attacker floods port on a remote host with numerous UDP packets and when the host checks for the packet, which is to be received at that port and when there is no legitimate packet found, it replies with an ICMP destination unreachable packet. This will ultimately lead to inaccessibility. The other attack is Ping of Death attack which involves the attacker sending numerous malformed packets or malicious pings to a computer which results in the overflow of memory buffers allocated for the packets causing the denial of service.

Intrusion detection system (IDS) discovers the intrusions in the network[10]. An intrusion detection system (IDS) is a software application that will monitor the network or system activities for malicious activities or policy violations and then it will produce the reports to the administrator.

There are two type of intrusion detection system

(i) Signature based intrusion detection

(ii) Anomaly based intrusion detection [11].

Signature based intrusion detection system maintains a database of signature of previously known attacks and match the signature of the newly captured data to monitor the intrusion in the network whereas anomaly based system do not rely on the prior knowledge of attacks it monitors the system activities for abnormal behaviour [12]. To detect the abnormal behaviour, the administrator should develop the detailed knowledge about the accepted behaviour.

II. PROPOSED SYSTEM

Mobile ad-hoc network is a self configuring network without a central system and each node works as the router hence it is more vulnerable to DDoS attack. Understanding the network routers and the path it takes to route the packets in a mobile ad-hoc networks is a major concern. There are different types of DDoS attack, but in this paper two DDoS attacks are being concentrated; that is UDP flood attack and Ping of Death attack. These attacks look very simple but it may cause a major damage to the network if it is neglected.

An intrusion detection system is developed to detect UDP flood attack and Ping of Death attack and secure the MANET from the same. This system helps us to identify the attacking node by the number of packets it sends.

III. METHODOLOGY

Algorithm to Detect UDP Flood Attack

STEP 1: Start

STEP 2: Identify nodes in network.

STEP 3: If nodes in range

STEP 4: Set THRESHOLD.

STEP 5: CAPTURE packets.

STEP 6: If packet not of standard type

Notify Malformed_ packet.

STEP 7: Identify UDP_PACKET.

STEP 8: If UDP_PACKET > THRESHOLD

Notify UDP_FLOOD_ATTACK

STEP 9: Stop

Algorithm to Detect Ping Of Death Attack

STEP 1: Start

STEP 2: Identify nodes in network.

STEP 3: If nodes in range

STEP 4: Set THRESHOLD.

STEP 5: CAPTURE packets.

STEP 6: If packet not of standard type

Notify Malformed_packet.

STEP 7: Identify ICMP_PACKET.

STEP 8: If ICMP_PACKET > THRESHOLD

Notify PING_OF_DEATH_ATTACK

STEP 9: Stop

The neighbouring nodes that are present in the network are checked at first. If the node belongs to the network and if it is sending packets to the network then the Intrusion Detection System will capture the packets from the network. The packet that is captured will be processed to know whether the packet is a UDP packet or an ICMP packet and also get the other necessary information about the packet. The IDS will keep a count of all the receiving packets. If the number of UDP packets received from a node is higher than the defined threshold, then it will notify about UDP flood attack and in the same way, if the number of ICMP packets received from a node is higher than the set threshold, the IDS will notify about the Ping of Death attack. The IDS will also show the list of nodes which are sending UDP and ICMP packets which will be flooding and pinging continuously to the node.

IV. Experimental Results

A. *Comparison between normal UDP packet flow and UDP flood attack*

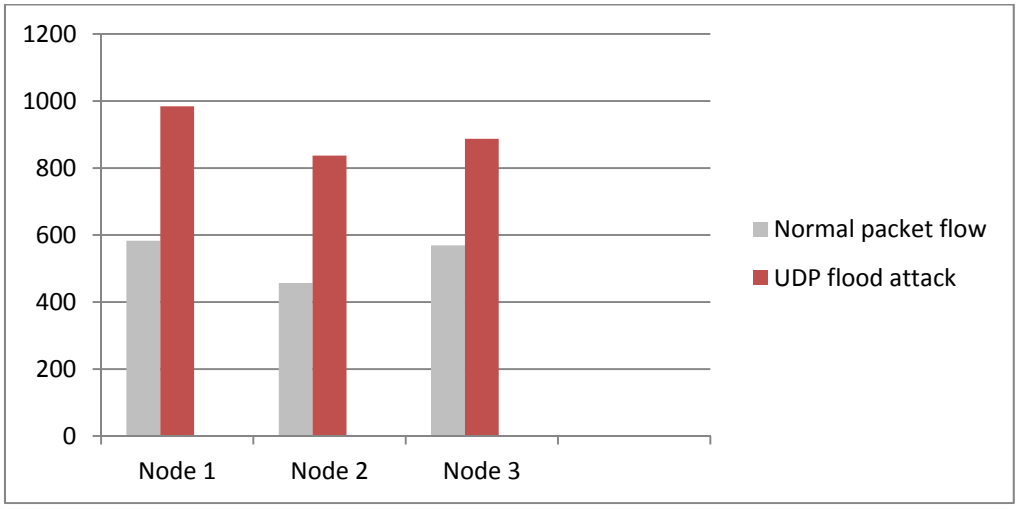

Fig 2 Comparison Between Normal UDP Packet Flow And UDP Flood Attack

B. Comparison between normal ICMP packet flow and Ping of Death attack

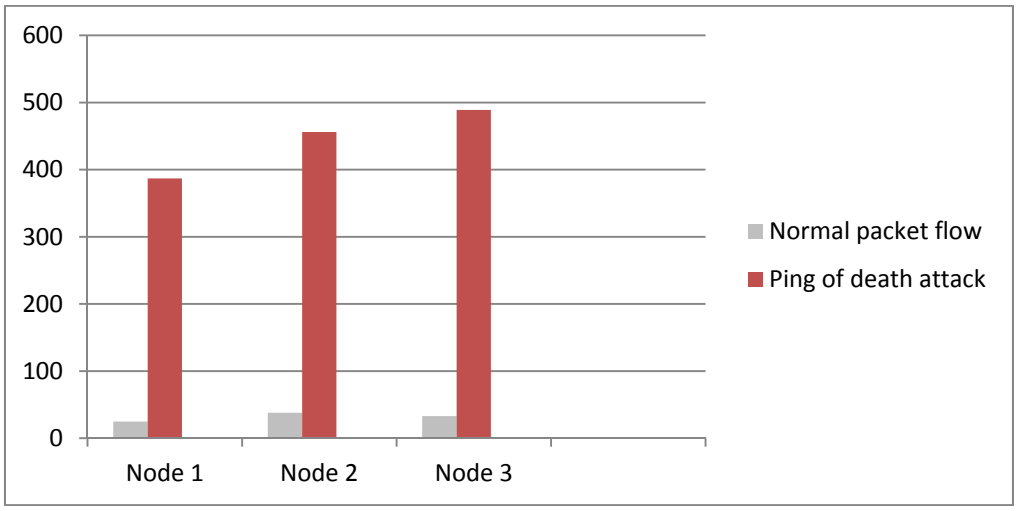

Fig 2 Comparison Between Normal UDP Packet Flow And UDP Flood Attack

The main concept here is to get the knowledge about the number of packets that arrive from the node to the IDS. The above depicted graph shows the reading about the normal packets that is received in a time interval of 30sec. Where the threshold for UDP flood attack was set to 700 and for Ping of Death attack the threshold is set to 300. The observation made, tells that the UDP flood attack and ping of death attack will definitely affect the network. During the attack it is observed that the routing load is very high because the attacker will try to flood and ping the victim node and the congestion occurs. Hence the packets will not be delivered accurately and the packet drop rate increases.

V. Conclusion

DDoS attacks make the nodes in mobile ad hoc network unavailable to the legitimate users. This research work concentrates on two kinds of DDoS attacks namely UDP flood attack and ping of death attack. These two attacks flood the victim nodes with unnecessary packets resulting in channel congestion and denial of service.

Intrusion detection systems are used to monitor the network for malicious activities or violations of policy. The intrusion detection system will identify the kind of packets and if the flow of packet in the node is more than the set threshold then it will identify the source node which is causing the UDP flood attack or the Ping of Death attack and notify about the attack.

VI. FUTURE WORK

Our analysis has concentrated on two main attacks in DDoS which seems to be simple but causes more damage to the network. The captured raw data is checked whether the size of it is according to the standard size. If the data captured is not according to the standard size then it can be called as the malicious or a malformed packet. In the future work the source address of these malicious or the malformed packets can be identified. If the source address of the node which sends malformed packets are identified then the network can be secured from such attacks to an extent.

ACKNOWLEDGMENT

We express our heartfelt gratitude to Mr. Gokul Dev.S, Chairperson, Department of Computer Science for his guidance and constant supervision as well as for providing necessary information regarding the project and also for support in completing the project.

We would like to express our gratitude towards our parents and members of the Department for their kind co-operation and encouragement.

Our special gratitude and thanks to all people for giving us such attention and time for completion of this project.

REFERENCES

[1] Prajeet Sharma, Niresh Sharma and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications, ISSN: 0975-8887, Volume 41, Issue 21, March 2012.
[2] Ankush pawar and Kshama Dwivedi, "Prevention against DDoS in MANET using IDS" International Journal of Application or Innovation in Engineering and Management, ISSN: 2319-4847, volume 3, Issue 12, December 2014.
[3] Jaganath and Premala Patil, "A Secured Intrusion Detection System Against Ddos Attack In Manets".
[4] Vikas Chouhan and Sateesh Kumar Peddoju, "Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing", Electronics & Computer Engineering Department, Indian Institute of Technology Roorkee, India.
[5] Chilakalapudi Meher Babu, Dr. Ujwal A. Lanjewar and Chinta Naga Manisha, "Network Intrusion Detection System on wireless mobile ad-hoc Networks", International Journal of Advanced Research in computer and communication Engineering, volume 2, Issue 3, March 2013.
[6] A. Anna Lakshmi and Dr. K.R. Valluvan, "A Survey of Algorithms for Defending MANETs against the DDoS Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Volume 2, Issue 9 September 2012.
[7] Stephen M. Specht and Ruby B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures".
[8] Shahid Akhter, Jack Myers, Chris Bowen, Stephen Ferzetti, Patrick Belko, and Vasil Hnatyshin, "Modeling DDoS Attacks with IP Spoofing and Hop-Count Defence Measure Using OPNET Modeler", Department of Computer Science Rowan University Glassboro.
[9] Anurag Kumar, Akshay Kumar, Anubha Dhaka and Garima Chaudhary "Intrusion detection against denial Of service attacks in MANET Environment", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), ISSN: 2278-6856, volume 2, Issue 4, July-August 2013.
[10] N. Sharmila Kumari, Santhosh Kumari, Apoorva. D and Mrs. Neelufar, "A study on intrusion detection system against DDoS attack in MANET", International Journal of Scientific and Research Publications, ISSN: 2250-3153, Volume 4, Issue 12, December 2014.
[11] V. Jyothsna and V. V. Rama Prasad, "A review on anomaly based Intrusion Detection System", International Journal of Computer Applications, ISSN: 0975-8887, Volume 28, Issue 7, September 2011.
[12] S. A. Joshi and Varsha S. Pimprale, " Network Intrusion Detection system (NIDS) based on Data Mining", International Journal of Engineering Science and Innovative Technology (IJESIT), ISSN: 2319-5967, Volume 2, Issue 1, January 2013.

AUTHOR PROFILE

Ankur Ashok Acharya is currently pursuing MCA from Amrita Vishwa Vidyapeetham University, Mysuru Campus and he has completed his BCA from Amrita Vishwa Vidyapeetham University, Mysuru Campus.

Arpitha K M is currently pursuing MCA from Amrita Vishwa Vidyapeetham University, Mysuru Campus and she has completed his BCA from MMK and SDM college, Mysuru

Santhosh Kumar B J has completed his M.Tech(I.T) from Karnataka State Open University (KSOU), Mysuru, Karnataka, M.Sc (SIS) from Bharathiar University, Coimbathore, Tamil Nadu, B.Sc (PMC) from Mysore University, Karnataka. Now he is working as Assistant Professor, Department of Computer Science, Amrita Vishwa Vidyapeetham University, Mysuru Campus.