Singh et al., J Comput Eng Inf Technol 2018, 7:5
DOI: 10.4172/2324-9307.1000214

Journal of Computer Engineering & Information Technology

Research Article

A SCITECHNOL JOURNAL

A Novel Technique to Defend DDOS Attack in Manet

Singh N[1]*, Dumka A[2] and Sharma R[3]

Abstract

Manet is highly vulnerable to distributed denial of service (DDOS) attacks; These DDOS attacks consume all system resources like battery power, bandwidth, energy, CPU resources, CPU cycles etc and also make resources or nodes unavailable to the legitimate users. Therefore these DDOS attacks always affect the network connectivity due to the dynamic nature of the nodes as well as functioning of the network which results in data delivery and packet dropping. Significant efforts have been made for the security of Adhoc network but it will not work always due to the dynamic behavior of nodes in the network. In this paper we will present a deep sight into DDOS attacks and how they affect the MANET, also how these attacks can be defended in the network and how we can make the network more secure by understanding the nature of attacks.

Keywords

Mobile adhoc networks (MANET); Denial of service (DOS); Distributed denial-of-service (DDOS); Dynamic nodes; Black hole attacks

Introduction

Since wireless sensor networks are not directly connected hence they are easily susceptible to attacks. The intrusion of the attacker in wireless network is very much easy as compared to wired medium so denial of service attack is more using frequency bands. The mobile ad hoc network increases the risk of vulnerabilities. The wireless networks or Ad hoc networks cannot be made secure using the facilities provided by equipment such as firewalls, authentication servers etc [1,2]. DDOS attacks in Manet are known to be a dangerous attack. It is a large scale attack over the network which blocks the services of the legitimate users. It takes place on victim system with large amount of data or victim machine with getting help or cooperation from various hosts which are all over the network [3]. Traffic from the attacker side engages the network resources so that legitimate requests will be discarded or will not be able to send or receive data or packets [4,5]. The Unwanted data in form of packets flooded the network of the user for the bandwidth depletion which blocks the data of user to reach its destination. The services of the legitimate user are closed due to the depletion in bandwidth and resources [6]. These type of attacks always target to any server or any victims process by making it unavailable for the genuine users. A large number of resources can be attacked by the attacker. The best way to protect the data or information is to design some detection or prevention techniques which can effectively detect the attackers and prevent it by blocking the attackers [7]. These attacks vary from small to large so they can destroy data completely or they can stop or block services to the user. These DOS attacks can destroy both networks at client side as well as at server side. For example, a dos attack can destroy legitimate users systems by tying them up which includes resources as bandwidth, energy, storage, scalability also it includes CPU cycle [8]. By just changing the route information or configuration of system an attack can take place in the network. Distributed denial of Service attacks will always be there in MANET or ad hoc networks. In this attack various systems in a network work together to attack a victim's system so that he may not get desired services, this denial of service attack (DOS) target a single system and his device or system is attacked with large amount of data in form of packets which results in blocking services of a legitimate users [9]. These attacks will affect the resources and efficiency of the victim and due to this service to legitimate users are unavailable and performance is highly degraded. This can be also termed as that Distributed Denial of Service (DDoS) attacks are those planned or we can say coordinated attack on the victim system on its available services with the help of many other compromised systems. DDoS attack basically consists of two phases i.e. Deployment Phase and Attack Phase. A DDoS attack in form of program is first being deployed on compromised hosts and then in next step attack is done. DDoS attacker always takes help from many computers to launch an attack on many targets simultaneously. Victims can be termed as primary and secondary like those who are under attack are called as "Primary victim" and others are called as "secondary victims". Role of secondary victim is to make the attack much larger and destructive by helping the attacker and remaining anonymous throughout the network.

Mobile Adhoc networks have two types of attacks:

- Active DDOS attack is an attack where attacker nodes have to loss some energy for performing the attack.
- Passive DDOS attack is an attack where nodes are not supporting or cooperative due to selfishness of saving their energy.

So the nodes which aim active DDoS attacks are always considered as attackers while nodes that are passive they considered as selfish for saving their resources or battery and DDOS attacks will occur. Several DDoS attacks were there, some against high-profile sites like CNN Amazon, yahoo in 2000 and also various attacks on GRC.com in 2001 and my doom virus attack on SCO website in Feb 2003. All these attacks show how massive and destructive these attacks can be and how they would lead to huge loss to the organization in terms of energy and cost.

Paper Organization

The background and related work is there in Section II, Proposed work is there in Section III, Section IV includes Experimental Results, and Section V shows the Conclusion. Referring different type of situation in the network consequences are mentioned in section VI under future scope and the proposed work may be extended further

Problem identification

- Congestion or traffic is created by attackers by dropping packets or by sending large amount of data which block

***Corresponding author:** Neha Singh, Research Scholar, Uttarakhand Technical University, Jharkhand, Dehradun, India, Tel: +91-9917155889; E-mail: singh.neha773@gmail.com

Received: November 05, 2018 **Accepted:** December 19, 2018 **Published:** December 22, 2018

legitimate users and they will not be able to send the data or packet to the desired nodes.

- Several DDoS detection techniques are unable to detect the attacks and can't differentiate them from legitimate users.

Background

Ad hoc networks are dynamic in nature and they can be formed when we do not have any communication infrastructure. MANET has node mobility and it also has limited characteristics like bandwidth, battery power, storage space and CPU cycle. We assume in MANET that the various intermediate nodes help in forwarding data packets. MANET has the property or capability of forming various changing network topologies without use of any centralized administration. The main concern or challenge in MANET is to provide better security. The performance and reliability of network in MANET is disrupted by various attacks [10]. The DOS and DDOS attacks result in the degradation of genuine use of network resources. The objective of the study is to be known about various services and how much it will affect the network functioning or operation. For the purpose of communication nodes of the network are used for that node information is required which is always secret [11,12]. This secret or confidential information captured by node always have issue of security. DDoS (Distributed denial of services) attack is one of the major threats in the network. DDOS attacks are done in the network by the attackers by suspending or interrupting the services of legitimate users. Therefore different methods or techniques are developed for the security [13]. So an analysis will be there for these types of DDOS attack, components of DDOS attack, need for prevention and detection techniques. (MANETs) permit various mobile hosts without any prefixed infrastructure to form a communication network which results into high flexibility but also it brings more challenges in MANET for fighting against attacks. The features of MANET like mobility and redundancy give new ideas to design detecting and preventing strategy. Sometimes it was assumed that an attacker node always target specific users or victims and also if the attacker fails to achieve its target after a specific amount of time then it will give up. In some defense strategy, the high redundancy can be used for selecting a secure node [14]. When a DDOS attack has been find out, the attacker or malicious traffic will be directed only towards the secure node and so the node of the victim can work as a normal node, then it can be expected that the attacker will not continue the attacking process meaninglessly. In mobile Ad Hoc Networks (MANET) each and every node work as a transmitter or router at such devices like switches, router, gateways total traffic monitoring can be done in wired networks but it is not possible in ad hoc networks [15]. For this various defensive or preventing schemes like neighbor monitoring, cluster based or trust building techniques have been proposed to find out the malicious nodes in the network. The various resources used by ad-hoc network nodes for monitoring, detecting, reporting, and diagnosing of malicious activity [16] (Figure 1).

Proposed Work

We have proposed a technique which can surely detect the DOS attacks in the network and for that purpose we have used various parameters which are very important for mobile ad hoc network and help nodes to send data packets from one node to another as it is known to us that MANET does not have base stations, everything is done from node level. So the different parameters or attributes which we have used to defend the DDOS attacks are as follows:

- RREQ: Each and every node will discover a route by sending RREQ request to find the availability of the node. A RREQ packets contains the following information like Source id(Sid), Destination id(Did), Source sequence no.(Ssq), Destination sequence no. (Dsq) and Time to live(TL)
- RREP: It act as an acknowledgement of route request (RREQ) and will response the node about the availability of the route.
- Throughput(Tth): Ratio of amount of data received to time taken by last packet to reach
- Packet delivery ratio: Ratio of packets successfully delivered to destination compared to packet sent. (pckt loss=pckt sent-pckt recieved)
- Energy consumption: Discard nodes which consume or waste more energy of the node
- Scalability: Don't allow the node which is more scalable

Mechanism

Send RREQ

If node=available then, Acknowledgement=RREP;

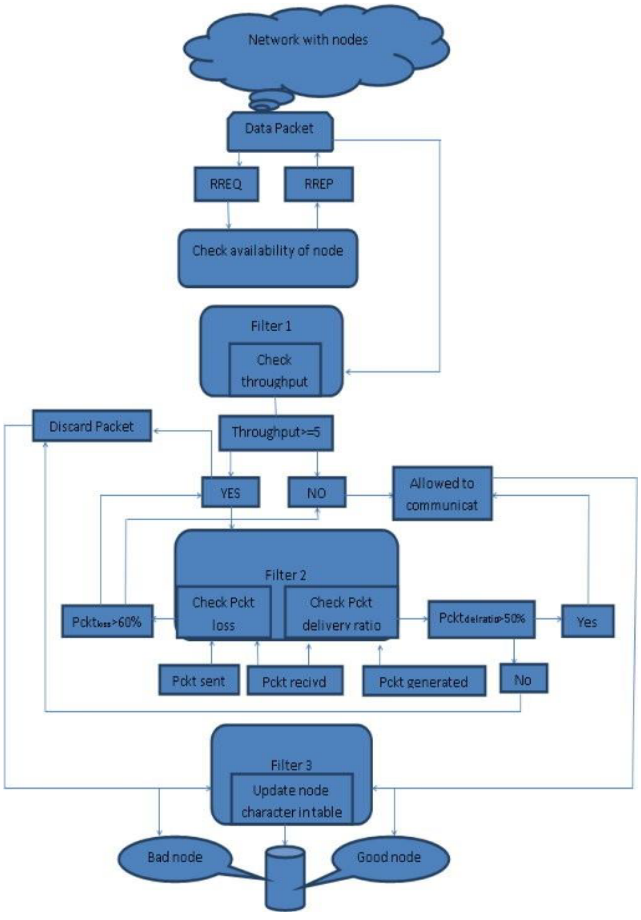

Figure 1: Architecture of proposed defending technique.

{

Filter 1:

Check throughput (0<=Thro>=10) If Thro>=5;

Forward Packet to filter2;

Else

Allow packet to communicate;

}

Filter 2:

Check Packet delivery ratio;

{

If Pckt(rec)/Pckt(gen) >50%; Check(Pcktloss);

{

Pcktloss=(Pcktsent-Pcktrec); If Pcktloss >60%;

Discard Packet (Bad Node); Else

Send Pckt to filter 3;

}

Else

Discard Packet (Bad Node);

}

Filter 3:

Enter node name or node number to the character

{

Good node Else

Bad node

}

Experimental Result

The simulator NS2 is used for simulation of Proposed Algorithm. Channel capacity of hosts is 2 Mbps. Our simulated settings are as below in Table 1 (Figure 1). The experimental set up is done with five different normal flow of traffic with data rate 50 kbps and data rate for attacking packets is 500 kbps. The proposed algorithm is compared with SWAN [3] and it can be observed that received bandwidth of proposed algorithm is greater than SWAN and result can be seen in Figure 2. Packets lost over a period of time can be seen in Figure 3. From the figure we can find out that packet loss for the proposed algorithm is less as compared to other scheme. Our technique made packet loss rate less in case of legitimate users. The result is also measured with variable attackers. In our proposed algorithm attackers are identified and blocked successfully so we can observe in (Figure 4) that we can achieve more bandwidth with more number of attackers. Packet delivery ratio is termed as number of packets received to total number of packets sent. Our proposed method will discard if packet delivery ratio is less but we can see that packet drop is reduced and more packets can be delivered to the destination. Result can be seen in Figure 5. In Figure 6 it can be observed that number of packets dropped of the proposed technique is less as compared to SWAN as attackers are blocked successfully.

Table 1: Simulation parameters.

Parameters	
No. of Nodes	80
Area Size	1200 × 1200
Mac	802.11
Radio Range	250m
Simulation Time	60 seconds
Traffic Source	CBR
Packet Size	512
Routing Protocol	AODV

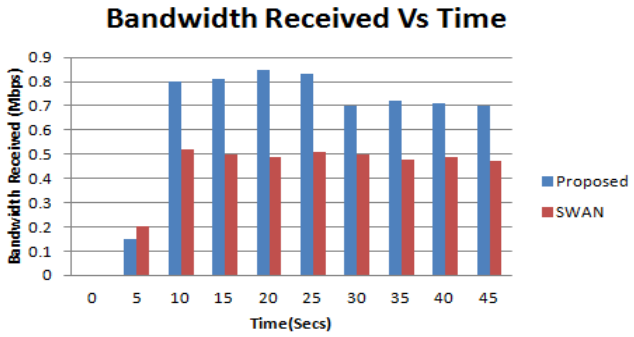

Figure 2: Bandwidth Received vs. Time.

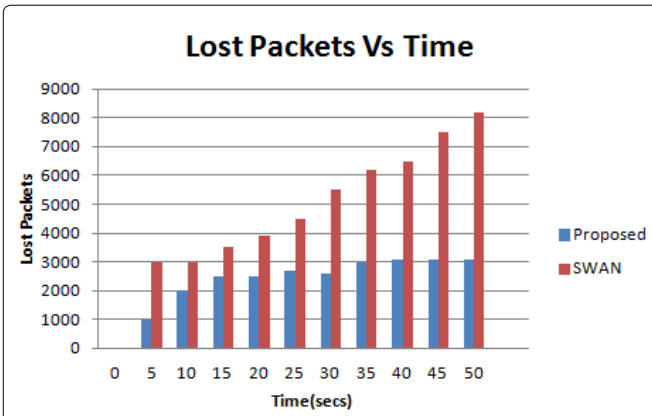

Figure 3: Lost Packets vs. Time.

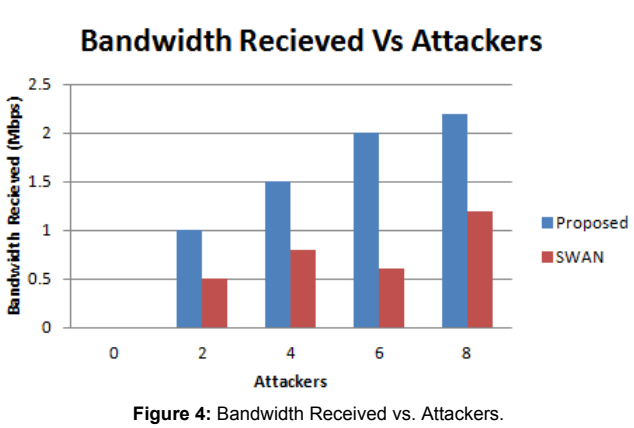

Figure 4: Bandwidth Received vs. Attackers.

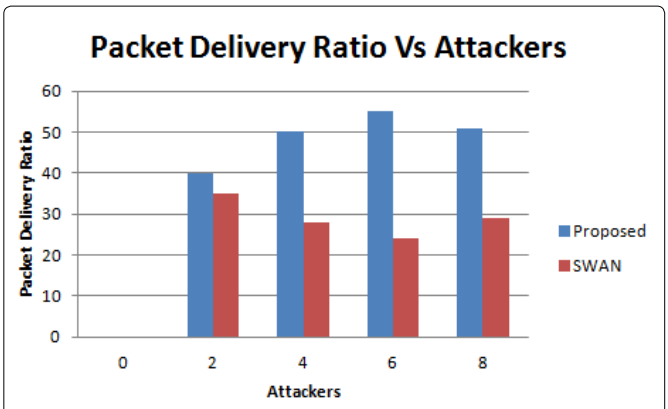

Figure 5: Bandwidth Received vs. Attackers.

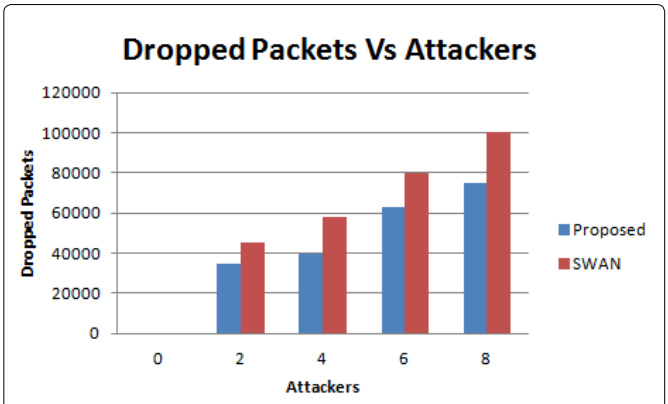

Figure 6: Dropped Packets vs. Attackers.

Discussion and Conclusion

In this paper, we have discussed about DDoS attacks and proposed an effective defense mechanism to provide security against attacks in mobile ad hoc network. Our Proposed algorithm provides rate limiting by identifying the attacking flows in the network. Once the attacker is identified that node or the traffic of that node is completely discarded which make the resources available for genuine users in the network and make the network more efficient. We have compared the performance of the proposed technique with the defense scheme SWAN and through results it is proved that our algorithm is better than existing. By results of simulation it can be seen that through our proposed technique bandwidth received, packet delivery ratio are high and packet loss is less.

Future Scope

In this paper, we have discussed about DDoS attacks and proposed an effective defense mechanism to provide security against attacks in mobile ad hoc network. Our Proposed algorithm provides rate limiting by identifying the attacking flows in the network. Once the attacker is identified that node or the traffic of that node is completely discarded which make the resources available for genuine users in the network and make the network more efficient. We have compared the performance of the proposed technique with the defense scheme SWAN and through results it is proved that our algorithm is better than existing. By results of simulation it can be seen that through our proposed technique bandwidth received, packet delivery ratio are high and packet loss is less.

References

1. Singh S, Chaudhary S, Vatsa AK (2012) Explicit query based detection and prevention techniques for DDOS in MANET. IJCA 53: 19-24.
2. Francois J, Aib I, Boutaba R (2012) FireCol: A collaborative protection network for the detection of flooding DDoS Attacks. IEEE 20: 1828-1840.
3. Ahn GS, Campbell AT, Veres A, Sun LH (2002) SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks. In: Proceedings of IEEE Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, 2.
4. Lu K, Wu D, Fan J, Toderovic S, Nucci A (2007) Robust and efficient detection of DDoS attacks for large scale internet. 10: 5036-5056.
5. Rana S (2011) Methodology for detecting and thwarting DoS in MANET. IJCA 1: 31-34.
6. Alicherry M, Keromytis AD, Stavrou A (2009) Deny- by-Default Distributed Security Policy Enforcement in Mobile Ad Hoc Networks 19: 41-50.
7. Kim M, Na H, Chae K (2004) A Combined Data Mining approach for DDoS attack Detection. Springer, 943-950.
8. Arunmozhi SA, Venkataramani Y (2011) DDoS Attack and Defense Scheme in Wireless Ad hoc Networks. IJNSA 3: 182-187.
9. Jia Q, Sun K, Stavrou A (2011) CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET. ICCN 143-147.
10. Bala K, Bansal A (2015) A Review on Mobile Ad-hoc Network with Attacks impact. IJIR. 1: 6-10.
11. Begum SA, Mohan L, Ranjitha D (2012) Techniques for resilience of denial of service attacks in mobile ad Hoc Networks". IJECCE 3: 152-156.
12. Kaur K, Singh BL (2015) Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Network. IJAST 82: 63-70.
13. Zanoon N, Albdour N, Hamatta HAS (2015) Security challenges as a factor affecting the security of manet: attack & security solutions. IJNCA 7: 1- 13.
14. Khamayseh Y, Al-Salah R, Yassein MB (2012) Malicious nodes detection in MANETs: Behavioral analysis approach. J Networks 7: 116-125.
15. Lamba A, Garg S (2015) A study on the behavior of manet: along with research challenges, application and security attacks. IJETTCS 4: 141-146.
16. Lovely (2015) Implementing DoS Attack Defence Scheme in Manet. IJARCSSE, 5: 522-526.

Author Affiliation Top

[1]*Uttarakhand Technical University, Dehradun, India*

[2]*Graphic Era (Deemed to be University), Dehradun, India*

[3]*Govt of Ranchi, India*