ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(33), DOI: 10.17485/ijst/2015/v8i33/80152, December 2015 ISSN (Online) : 0974-5645

Detection and Defense Mechanism against DDoS in MANET

Tariq Ahamad* and Abdullah Aljumah

College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, AlKharj, Saudi Arabia; t.ahanger@psau.edu.sa, aljumah@psau.edu.sa

Abstract

DDoS is a serious issue and a ruthless attack in the networks that need to be detected and defended before reaching its target and causing the damage for user, data and the services. So, it is extremely important to prevent DDoS attack rather than letting it occur and then defending it. In this article we have used Reply Request (RREQ) with a thresh hold time mechanism to deal with this threat. We have used calculations and their analysis to detect the threat and the malicious node and with the help of reply request with thresh hold time we have proposed a detection technique and we can detect the malicious data source node as well. In this research we have evaluated the robustness of existing routing protocols against the malicious attacks and assess the quality and impact of security improvements and have proposed a reliable solution to handle DDoS attacks in MANETS.

Keywords: Ad Hoc, Black Hole, DDoS, MANET, Security

1. Introduction

The concept of Mobile Ad Hoc Network (MANET) depends on the availability of the devices that are to be connected to each other to form the network. Thus, unlike other existing and traditional networks, these networks do not depend on any pre-existing network or infrastructure to carry out their operations and their dynamic character reduces their cost and implementation time[1,2]. Figure 1 illustrates the basic structure of Mobile Ad Hoc Networks.

The backbone of the Mobile Ad Hoc Network is the routing protocols that enable multi – hop data transfer or communication in these networks[3]. Since the topology of these dynamic networks keep on changing so changes the attacks on these networks and in order to deal with these malicious attacks these routing protocols must be robustic[4]. The pre-existing routing protocols easily deal with changing topologies but the malicious attacks always remain the issue to be fixed.

2. Threats in Mobile Ad Hoc Networks

Reliability of the devices or nodes that are to be used to form a Mobile Ad Hoc Network is most important concept to be kept in mind as devices or nodes act both as computers and routers. Since the topology keep on changing due to dynamic behavior of the network, this change is supported by routing protocols so as to establish the dynamic routes[5]. Since routing information is very sensitive and can be targeted by the attackers in order to harm the network or the applications running in the network as illustrated in the Figure 2.

Since all the Ad Hoc Networks thoroughly depends on routing protocols, there are many sources that make use of this idea and attack them and the two major sources are:

- As per the basic cyber attack practice, the first comes from explicit attackers. By inserting a new large pool of routes or using old routing information or distract-

* Author for correspondence

ing the current routing pool, an intruder can divide the network or delay the traffic and can cause inefficient routing and affect the quality of service (QoS)[6].

- The most dangerous and that can cause severe effect to the dynamism and reliability of Ad Hoc Network comes from inside the network by grey nodes (compromised nodes) and can exploit the routing information of the other nodes and can affect the service as they are the part of the network[7].

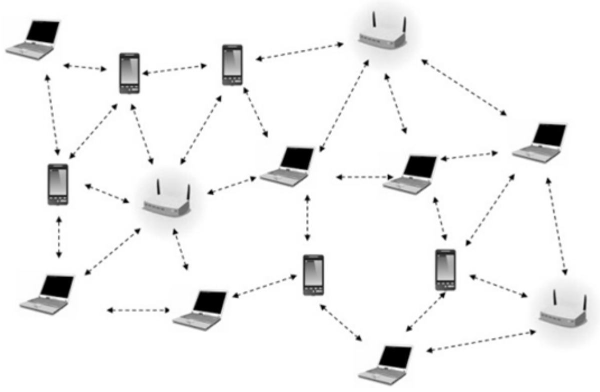

Figure 1. Mobile Ad Hoc Network.

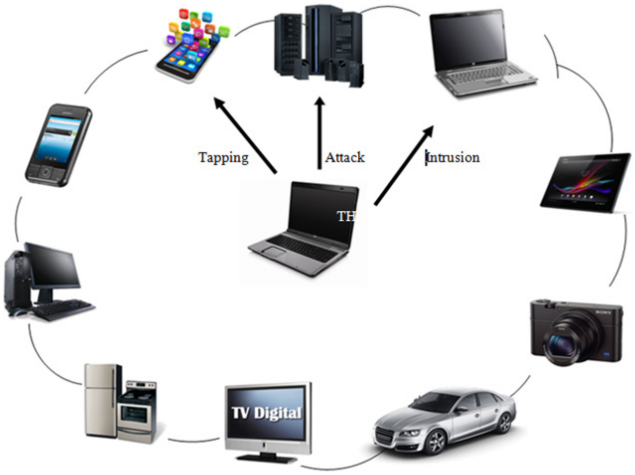

Figure 2. Attack in Ad Hoc Network.

3. Distributed Denial of Service Attack (DDoS)

DDoS is an attack to make an online service inaccessible by flooding it with malicious traffic from multiple sources and directions. So, a multitude of compromised computers attack a single system and cause the Denial of Service (DoS) for legitimate users of the victim node[8]. The data flood to the victim systems essentially compels it to shut down and this making the service unavailable for its legitimate users. A large number of computer hosts are controlled by the attacker before attacking the target node[9]. These machines are vulnerable in public networks and their weaknesses are exploited by the attacker through inserting malicious code or by using hacking techniques, so that the attacker can control them. The number of these compromised machines can be hundreds and thousands. These computers are called zombies and act as attackers agent[10]. The power and magnitude of attack is determined by botnet. So "the more botnet, the powerful will be the attack".

The attackers prepare a handler with botnet in order to control the zombies and this handler orders them and the zombies attack the target. The handlers also collect the information of the victim received through zombies. A typical Distributed Denial of Service (DDoS) attack architecture is shown in the Figure 3.

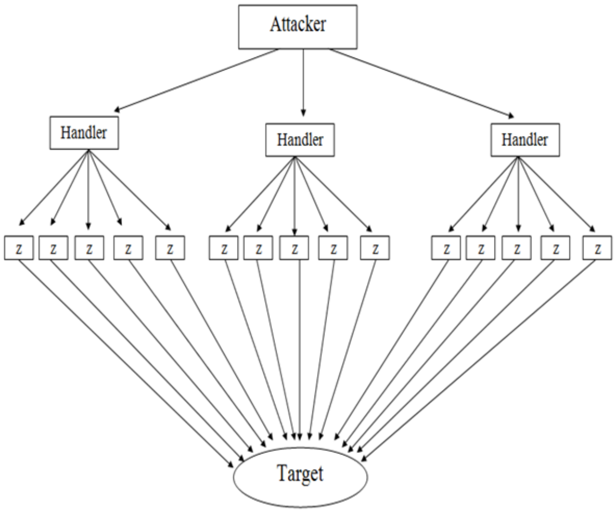

Figure 3. Distributed Denial of Service (DDoS) attack architecture.

DDoS becomes very hard to deal with when it occurs in unguided networks because of their changing topology, update frequency, low battery life, scalability, multicast routing, power aware routing, agent based routing etc.

4. Proposed Solution

In a broadcast, data packet is sent and delivered to multiple hosts and can be done at two OSI layers i.e. data link layer and network layer. The broadcast that is done at data link layer, packet are delivered to all the nodes attached to a specific physical network but the data packets broadcasted to network layer are delivered to all the attached hosts of a specific logical network.

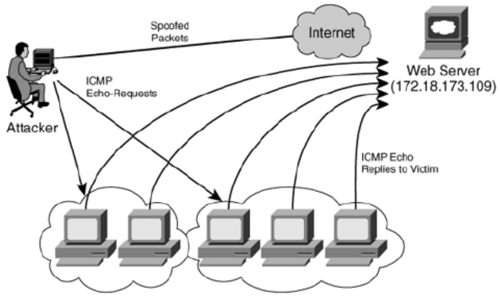

Figure 4. ICMP flood attack.

In a broadcast, all the data packets are to be delivered to all the hosts, the main job of a router is this situation is to check and control needless proliferation of packets (broadcasted packets). Usually routers support two types of broadcasting i.e., directed and flooded. Directed broadcast is a broadcast where packet are sent to a particular network or group of networks where as in flooded broadcast data packets are send to all the networks or every node of a network.

DDoS is caused with the help of flooding broadcast and a serious one among various DDoS attacks is SMURF attack than can be made possible usually because of the network nodes or devices which responds to ICMP echoes used to broadcast addresses. The attacker send a huge number of ICMP data packets to broadcast address

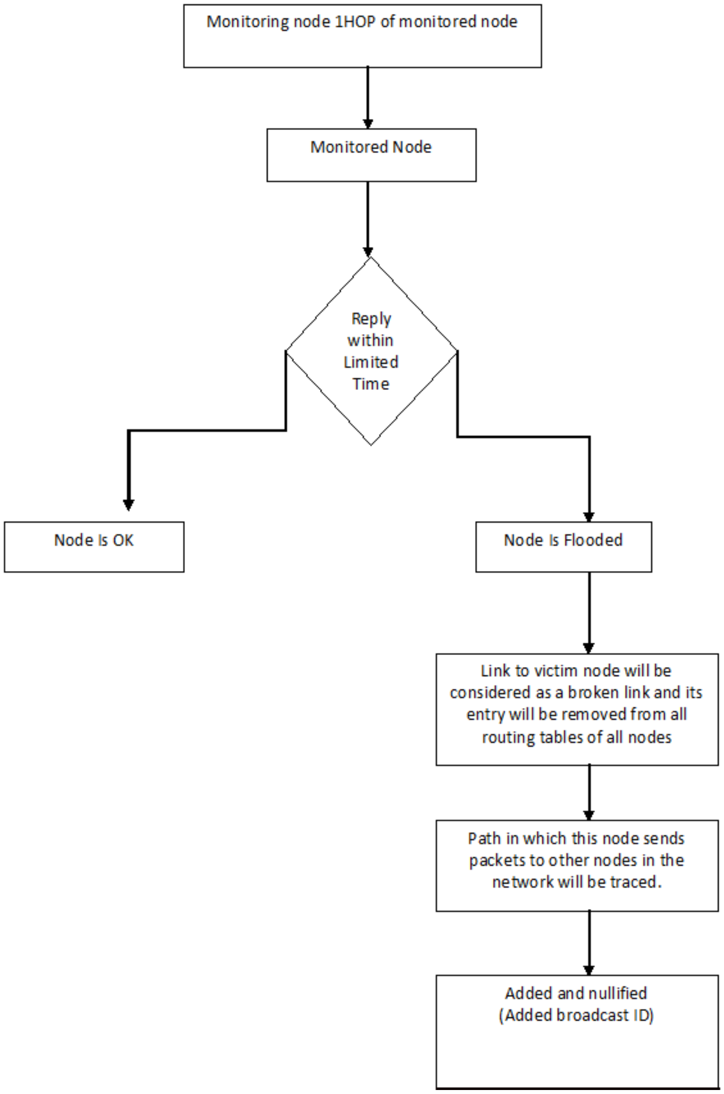
Monitoring node 1HOP of monitored node
Monitored Node
Reply within Limited Time
Node Is OK
Node Is Flooded
Link to victim node will be considered as a broken link and its entry will be removed from all routing tables of all nodes
Path in which this node sends packets to other nodes in the network will be traced.
Added and nullified (Added broadcast ID)

Figure 5. Proposed mechanism against DDoS in MANET.

and use the target victims IP address as source IP so that the replies from all the responding nodes will flood the victim node. The most important and surprising fact if this attack is that the attackers use a low bandwidth connection to target and kill high bandwidth node and its connection. The amount of data traffic that is sent by the attacker gets multiplied by the value equal to the total number of host nodes that reply to the ICMP echoes behind the router. Figure 4 illustrates the attack.

AODV routing protocols are used in IP broadcast to broadcast RREQ on all the host in a wireless network usually MANET to initiate RREQ packets in the MANETs, so that it becomes congested and no bandwidth will be available to send any kind of data packets. So, we need to check the exact number of RREQ's which are broadcasted or to be broadcasted to the nodes.

In our proposed detection mechanism, each and every node comes into processing. Figure 5 is a flowchart that describes our proposed mechanism against DDoS in MANET.

In this mechanism for each and every attack there will be a monitoring node that runs the corresponding detection rule and one whose behavior is being analyses (misbehaving or attacking node) is monitored node. The monitored node 1HOP of the monitoring node and can identify the attack type and attacker. A small packet “REP” will be sent by the monitoring node to its 1HOP (neighboring node) and have to wait for reply. In case, it doesn't get the reply within the specified time (threshold time) then the node is flooded node (target or victim node). After detecting this, its ID (attacked or victim node) will be disabled and will be deleted from the routing table of all nodes. After this step of finding the victim node, we can find the path that is used to attack and sum all nodes whose effect and damage will be nullified. The code of the procedure will be implemented in neighboring function, get-broadcast-id function and finally decide the function of aodv.pc file.

5. Conclusion

The proposed approach is based on reply request with thresh hold time in MANETs sent to 1Hop node in a particular sequence to detect the malicious behavior and based on its reply time taken to complete the reply-request loop its IP address can be added or removed from the routing table of the nodes of the network in order to keep the network safe from this attack. With this approach we can easily find the attacker and the target or victim node. This technique can be further analyzed and can be improved.

6. Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia during the academic year 2015/2016 under research number 2015/01/3850.

7. References

1. Uddin M, Alsaqour R, Abdelhaq M. Intrusion detection system to detect DDoS attack in gnutella hybrid P2P Network. Indian Journal of Science and Technology. 2013 Feb; 6(2):71–83.
2. Tamilselvan L, Sankaranarayanan V. Prevention of blackhole attack in MANET. 2nd International Conference on Wireless Broadband and Ultra Wideband Communications: Sydney, Australia; 2007 Aug 27-30. p. 21.
3. Raj PN, Swadas PB. DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. International Journal of Computer Science. 2009; 2:54–9.
4. Abdelhaq M, Hassan R, Ismail M. A study on the vulnerability of AODV routing protocol to resource consumption attack. Indian Journal of Science and Technology. 2012 Nov; 5(11):3573–7.
5. Wang W, Bhargava B, Linderman M. Defending against collaborative packet drop attacks on MANETs. 2nd International Workshop on Dependable Network Computing and Mobile Systems: New York, USA; 2009 Sep. p.1–6.
6. Sun B, Guan Y, Chen J, Pooch UW. Detecting black-hole attack in Mobile Ad Hoc Networks. 5th European Personal Mobile Communications Conference: Glasgow, United Kingdom; 2003 Apr 22-25. p. 490–5.
7. Khamayseh Y, Bader A, Mardini W, Baniyasein M. A new protocol for detecting black hole nodes in Ad Hoc Network. International Journal of Communication Networks and Information Security (IJCNIS). 2011 Apr; 3(1):36–47.
8. Tsou PC, Chang JM, Lin YH, Chao HC, Chen JL. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. 13th International Conference on Advanced Communication Technology: Seoul; 2011 Feb 13-16. p. 755–60.
9. Baadache A, Belmehdi A. Avoiding black hole and cooperative black hole attacks in Wireless Ad hoc Networks, International Journal of Computer Science and Information Security. 2010; 7(1):10–6.
10. Wang W, Bhargava W, Linderman M. Defending against collaborative packet drop attacks on MANETs. 28th International Symposium on Reliable Distributed Systems. 2009 Sep; p. 1–6.