Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1024 – 1030

RESEARCH ARTICLE

Security against DDoS Attacks in MANETs

Kulbir Kaur Waraich[1], Ranjeet Kaur[2]

[1]M.Tech (CSE) Student, DAV University Jalandhar, Email: - sbmk91@gmail.com

[2]AP in dept. of CSE, DAV University Jalandhar, Email: er.ranjeetsandhu@gmail.com

ABSTRACT:
As mobile ad hoc network applications are deployed, security emerges as a central requirement. In MANET, routing attacks are particularly serious. In this paper, the state-of-the-art of security issues in MANET is examined. The wireless ad hoc networks are highly susceptible to distributed denial of service (DDoS) attacks because of its unique characteristics such as open network architecture, shared wireless medium and no centralized controller and infrastructure. In this paper, the DOS attack, a severe attack in ad hoc networks that is particularly challenging to defend network's routing susceptibility is introduced and the network performance under two types of attacks, flooding attack and black hole attack that can easily be employed against the MANETS is analyzed and some methods are discussed to overcome these methods.

Keywords: MANET, DDOS, Flooding attack, Black hole attack.

INTRODUCTION

A MANET is a self-configuring network of mobile devices connected by links. Mobile hosts join on the fly and create a network on their own. With the network topology changing dynamically and the lack of centralized network management functionality, these networks tend to be vulnerable to a number of attacks. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure.

DDOS Attack:

A DOS attack is an attempt to prevent legitimate users of a service or network resource from accessing that service or resource. A Distributed Denial-Of-Service (DDoS) attack is a distributed, large-scale attempt by malicious users to flood the victim network with an enormous number of packets. This exhausts the victim network of resources such as bandwidth, computing

© 2014, IJCSMC All Rights Reserved

power, etc. The victim is unable to provide services to its legitimate clients and network performance is greatly deteriorated.

DOS attacks can cause a severe degradation of network performance in terms of the achieved throughput and latency. The performance of the wireless network is degraded by DOS depends on many factors such as location of malicious nodes, their traffic pattern, fairness provided in the network resources. The main aim of a DoS attack is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself.

1. Security attacks In MANET

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

1.1 External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network [1] The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

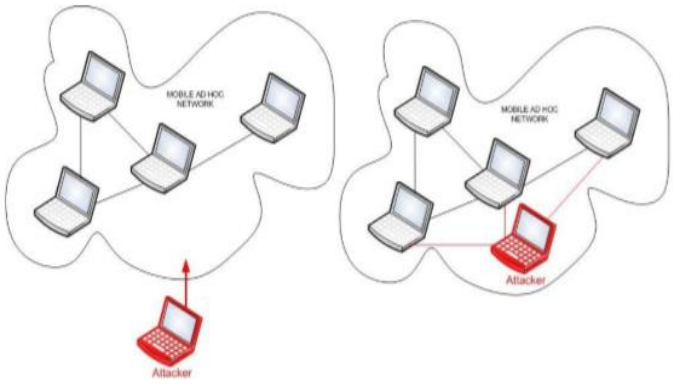

Fig1.External and Internal attack

1.2 Active and Passive Attack

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. These attacks are meant to destroy the performance of network. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network. [2]In Passive attack, the attacker listen to network in order to get information, what is going on in the network? It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

© 2014, IJCSMC All Rights Reserved

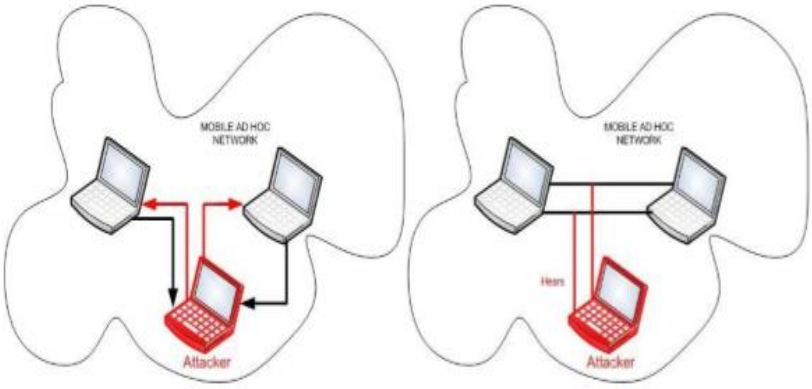

Fig2.Active and Passive attack

2. Overview of Selected Attacks

2.1 Blackhole Attack

In a Blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker [3] Therefore, all traffic will be routed through the attacker, and there- fore, the attacker can misuse or discard the traffic.

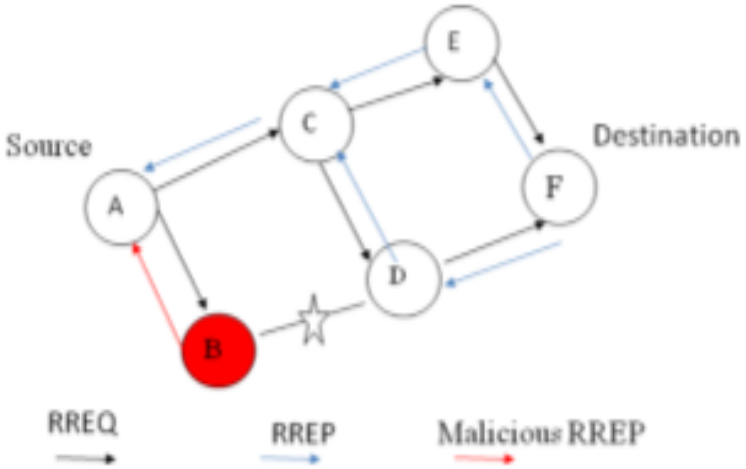

Fig3. Blackhole Attack

2.1.2 Black Hole Attack Caused By RREQ

An attacker can send fake RREQ messages to form Black hole attack [4]. In RREQ node address. Other nodes will update their route to pass by the non-existent node to the destination node As a result; the normal route will be broken down. The attacker can generate Blackhole attack by faked RREQ. The attacker forms a Blackhole attack between the source node and the destination node by faked RREQ message as it is shown in Figure 1

© 2014, IJCSMC All Rights Reserved

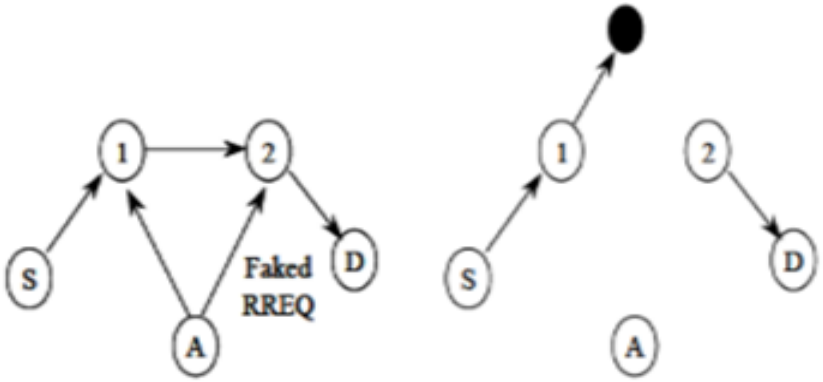

Fig 4. Blackhole caused by faked RREQ

2.1.2. Blackhole Attack Caused By RREP

The attacker unicasts the faked RREP [5] message to the originating node. When originating node receives the faked RREP message it will update its route to destination node through the non-existent node. Then RREP Blackhole [4] is formed as it is shown in Figure 2.

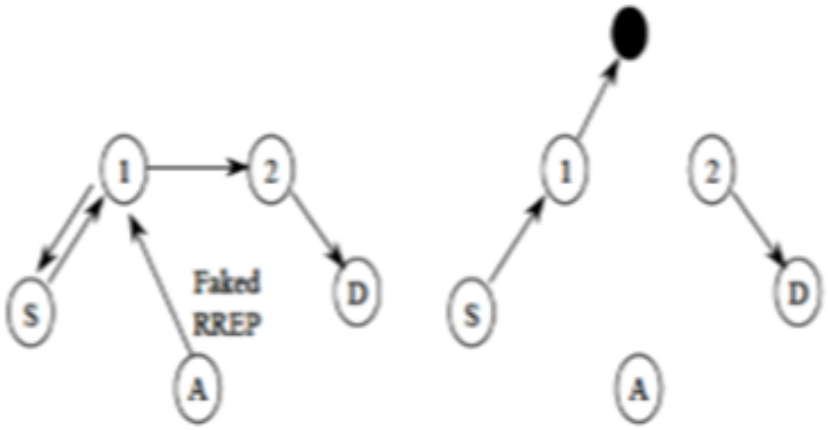

Fig 5. Blackhole caused by faked RREP

Difference between Attacks caused by RREP and RREQ

Table 1. Black hole attacks caused by RREP and by RREQ as discussed. [6]

Caused by RREQ	Caused by RREP
Set the initial IP address in RREQ to the IP address of source node.	Set the initial IP address in RREP to the IP address of source node.
Set the destination IP address in RREQ to the IP address of destination node	Set the destination IP address in RREP to the IP address of destination node
Set the destination IP address of IP header to broadcast address	Set the destination IP address of IP header to the IP address of node that RREQ has received
Set the source IP address of IP header to its own IP address and put high sequence number and low hop count in the RREQ field	Set the source IP address of IP header to its own IP address

© 2014, IJCSMC All Rights Reserved

2.2 Flooding Attack

The flooding attack is the most common attack found in Manet. The aim of the flooding attack is to exhaust the network resources such as bandwidth and to consume a node's resources or to disrupt the routing operation to degrade the network performance. This leads to a kind of Denial-of- Service (DoS) attack. The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [7]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources.

2.2.1 RREQ Flooding Attack

In this type of flooding attack, the attacker broadcast many RREQ packets for the node which exist or not exist in the network. To perform RREQ flooding the intruder disable the RREQ rate so it will effect on to consumes network Bandwidth. Generally all nodes have a limit beyond which requests cannot be sent. A node can not originate more than RREQ_RATELIMIT RREQ messages per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, up to a maximum of retry times at the maximum TTL value. [8] Repeated attempts by a source node at route discovery for a single destination must utilize a binary exponential back off. The first time a source node broadcasts a RREQ, it waits roundtrip time for the reception of a RREP. If a RREP is not received within that time, the source node sends a new RREQ.

2.2.2 Data Flooding Attack

When nodes in MANET find the correct routing path, source nodes send the data packets through that route. In data flooding attack, the attacker first maintains the routes to destination node, then sends frequently the useless data packets. The destination node will then be engaged in receiving the excessive data packets from the attacker and cannot work properly. The attacker packets engage the network and stop the processing of legitimate data packets.

3. Defense Schemes against selected Attacks

To prevent from these two attacks, the defense mechanism is proposed. This defense mechanism will detect these attacks and will provide secure channel to prevent against the threats.

3.1 Defense Scheme against Blackhole attack

It includes two steps

3.1.1 First Step: To resist the black hole attack, a neighborhood Route Monitoring Table (NRMT) is maintained by each node in the network. The NRMT maintains packet routing information of its neighbor nodes.[10] It contains the source ID, destination ID, source sequence number, destination sequence number, and a threshold value of sequence number which is dynamically updated, the time at which RREQ packet enters the node (RREQ-IN-TIME), the time at which RREQ packet leaves the node (RREQ- OUT-TIME), the time at which RREP packet enters the node (RREP-IN-TIME) and the time at which RREP packet leaves the node (RREP-OUT-TIME).

If the node is the normal node, once it receives the RREQ packet, it checks its routing table to identify whether it is the destination or not. If it is the destination node, it will send the RREP packet to the source node through its route or it will forward the RREQ to its one hop neighbor. Checking the routing information from the table requires a minimum time period known as MIN-TIME. If the node is the black hole node, it will send a RREP message without checking the table.

© 2014, IJCSMC All Rights Reserved

The NRMT maintains the record of the time of Reply. The first step of the detection process is based on the timing information of NRMT. Every node in the network when it receives the RREP from its neighbor, finds DIFF-TIME which is the difference between the RREQ-OUT-TIME and RREP-IN-TIME and compares this with MIN- TIME. If the RREP is from the black hole node DIFF-TIME will be less than the MIN-TIME. The node is identified as a suspicious node.

3.1.2 Second Step: As the second step of detection mechanism, RREPs sequence number is compared with the threshold value of sequence number. If the current sequence number is greater than the threshold value the node is confirmed as black hole and it is eliminated from the routing table. Once a node is detected to be really malicious, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources.

3.2 Defense Scheme against Flooding Attack

In this scheme, 2 steps are carried out for resisting the RREQ flooding attack.

3.2.1 First Step: In the first step, each neighboring node checks the time to wait for the RREP follows the binary exponential back off. [11][12]The nodes which do not obey this back off are identified as the suspicious node. The nodes then perform the second step of defense scheme.

3.2.2 Second Step: In this second step, the RREQ rate is checked. Here, two threshold values are maintained. The RREQ_RATELIMIT is considered as the upper threshold (UT) and RREQ_RATELIMIT /2 is taken as lower threshold (LT). [11][12] If RREQ rate is less than LT, the node which forwards the RREQ is identified as the normal node. If the RREQ rate lies between LT and UT, the forwarding node is identified as the suspicious node. The RREQ is then delayed in a queue. If RREQ rate is above UT, the forwarding node is identified as the attacker and the RREQ are dropped.

Hence, the attacking node is isolated from the network.

To resist the data flooding, in this paper, a new defense mechanism that maintains the flow Information monitoring table (FIMT) is analyzed. It contains flow id, source id, packet sending rate and destination id. Sending rates are estimated for each flow in the intermediate nodes. The updated flow information is sent to the destination along with each flow. The destination node sends the control message to notify the sender nodes about the congestion. The sender nodes, upon seeing these packets, will then reduce their sending rate. If the channel continues to be congested because some sender nodes do not reduce their sending rate, it can be found by the destination using the updated flow details. It checks the previous sending rate of a flow with its current sending rate. When both rates are same, the corresponding sender of the flow is identified as an attacker. Once the DDoS attackers are identified, all the packets from those nodes will be discarded. The attacker is blocked from the communication. Hence network resources are made available to the legitimate nodes in the network.

4. Performance Matrices

Performance Metrics We evaluates mainly the performance according to the following metrics.

4.1 Network throughput

A network throughput is the average rate at which message is successfully carried between source node and destination node. [9] It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination.

© 2014, IJCSMC All Rights Reserved

4.2 End-to-End delay

End-to-end delay is the average time that starts in the first node by generating the packets till the arriving the packets in destination node which shown in seconds. This delay includes the overall delay in the networks (i.e. buffer queues, transmission time and so on).

4.3 Network load

Network load is a major parameter with large effect on networks protocols that referred to the overall load that is impacted by the whole higher layer in all WLAN nodes in the network.

4.4 Latency

The latency is averaged over all surviving data packets from the sources to the destinations. It is the ratio of the number of packets received successfully and the total number of packets transmitted.

5. Conclusion

In these paper mainly two types of DDoS attacks such as flooding attack and black hole attack is analyzed. Also the Defense Schemes against these two attacks are discussed. For resisting the data flooding attack, a FIMT scheme was developed based on the flow information. The NRMT scheme for MANETs that is resistant to the black hole attack is developed. The scheme identifies the attacker based on timing information and destination sequence number.

References

[1] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[2] Bouam and Z. Othman. "Securing Ad Hoc Networks". IEEE Network magazine, special issue on networking security, November/December 2003, Volume 13, Issue, 6.

[3] Z. Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[4] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA

[5] H.Weerasinge and H.Fu (2008) "Preventing Black Hole Attack in Mobile Ad hoc Networks: simulation, implementation and evaluation "international journal of software engg. And its applications, vol2, no3

[6] Deborah Estrin, Lewis Girod, Greg Pottie, and Mani Srivastava. Instrumenting the world with wireless sensor networks. In International Conference on Acoustics, Speech, and Signal Processing, 2001.

[7] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[8] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. And Networking Conf., New Orleans, LA, 2005.

[9] N.V Trang and X.Xing "Rate–adaptive Multicast in MANETS" WiMob'2005, Volume 3, Issue, 19 pp. 352-360.

[10]S.A.Arunmozhi and Y.Venkataramani, A Flow Monitoring Scheme to Defend Reduction-of- Quality (RoQ) Attacks in Mobile Ad-hoc Networks, Information Security Journal: A Global Perspective, Vol.19, No.5, 2010, pp. 263- 272.

[11] Jelena Mirkovic and Peter Reiher, D-WARD: A Source-End Defense against Flooding Denial- of-Service Attacks, IEEE Transactions On Dependable And Secure Computing, Vol. 2, No. 3, 2005, pp. 216-232.

[12]Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks, IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, May 2010, pp. 579-582.

© 2014, IJCSMC All Rights Reserved