Malicious Attack on MANET using Maximum Segment Size

(IJCSNT) International Journal of Communication Systems and Network Technologies
ISSN Number: 2053-6283
Volume 4, Issue No. 1, 18–25

https://journals.mirlabs.in/index.php/ijcsnt
DOI-10.18486/ijcsnt/4.1.046

Laxmi Dike[1], Abhilash Sonker[2]

Abstract

MANET is an infrastructure less wireless network of Mobile Nodes connected directly or indirectly. It was basically designed for military purpose but now a days it is widely used in almost every field because of its characteristics. Wide scope of use has increased its vulnerability towards Malicious Attack. The attacks are particularly performed to reduce its throughput. We have considered Packet Deformation, a kind of Malicious Attack, caused by keeping variable Maximum Segment Size at intermediate nodes. Network Parameters are evaluated at presence and absence of Malicious Behavior. We have considered three parameters to view the effect of Malicious Attack namely, Throughput, End to End Delay and Jitter. On varing Maximum Segment Size, Packet Deformation causes changes in these parameters.

Keywords

Malicious Attack, MSS, Packet Deformation, Malicious Node.

Received: 10 December 2014; **Revised:** 12 March 2015; **Accepted:** 21 April 2015;
Published: 29 April 2015;

[1, 2]Computer Science and Engineering Department, Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh, India.

Corresponding author:
Email: laxmi.dike87@gmail.com

Introduction

MANET is infrastructure less, open environment network of Mobile nodes, self organized with dynamic topology. It was basically designed for uneven terrain where infrastructure was not possible like military camps [1,2]. But later on because of its easy configuration it was widely accepted in almost every field. Because of its wide use security became a major concern. Its open environment, wireless link, lack of clear line of defense, cooperativeness made it vulnerable for easy attacks. Many Intrusion detection systems are proposed for handling these attacks.

In this paper, we have launched an attack by varying Maximum Segment Size at intermediate nodes. This will deform the packet as it travels the route and thus will affect network performance.

The rest of the paper is organized as follows. Section II describes Security Attacks in MANET, Section III describes deformation of packet, Section IV describes Experimental Setup, Section V describes Data Analysis and Section VI is Conclusion.

Security Attacks in MANET

Attacks on MANET can either be classified as External vs Internal or Active vs Passive Attack. As it is very easy for nodes to enter in network therefore it is very easy to launch attack. External Attacks are caused by outsider who is not a member node, whereas Internal Attacks are launched by member node themselves, therefore it is very difficult to detect internal attack. On the other hand, Active and Passive attack are classified on basis of behavior of attack. When attack does not harm network, it either eavesdrop or monitors the network then it is Passive Attack. When the attacker's sole intention is to harm the network as flooding the network with control packet or beacon packet, dropping up of packet, modifying packets, are all Active Attacks. Some of the attacks on MANETs are Wormhole attack, black Hole attack, Jellyfish attack, Traffic Monitoring, Eavesdropping, Denial of Service, Rushing attack, Sybil attack, Session Hijacking etc. [3–5].

The attacker can be either Malicious or Selfish. As nodes themselves perform network functions in MANET, performing these network functions consumes significant amount of energy of member nodes. Selfish Nodes are unwilling to spend their energy in those functions which are not directly associated with them. They have no intention of harming the network. Malicious Nodes on other hand, intentionally harm the network by actively spending their resources. [6]

Deformed Packet

We are attacking the network by varying Maximum Segment Size of intermediate nodes. This is an active internal Attack performing Malicious behavior where attacker affects the Network Performance. Maximum Segment Size (MSS) is kept same at receiver and transmitter to avoid fragmentation and reassembly. If MSS is different at sender and receiver than the smaller amongst two MSS is chosen for transmission of packet. MSS is defined as "The maximum number of data octets that may be received by the sender of the TCP option in TCP segments with no TCP header options transmitted in IP datagram with no IP header options" [7]. MSS announcement is done from receiver to the sender that it can accept X amount of data. This X is MSS which can be larger or smaller than default MSS.

MSS can be calculated as [8]:

MSS = MTU - sizeof(TCPHDR) - sizeof(IPHDR)

Where MTU is maximum transmission unit and is determined through PMTUD (Path MTU Discovery). "Path MTU Discovery (PMTUD) is a standardized technique in computer networking for determining the maximum transmission unit (MTU) size on the network path between two Internet Protocol (IP) hosts, usually with the goal of avoiding IP fragmentation"[9]. On receipt of the MSS option the calculation of the size of segment that can be sent is:[8]

SndMaxSegSiz = MIN((MTU - sizeof(TCPHDR) - sizeof(IPHDR)), MSS)

There are three reasonable positions to take[8]: the conservative, the moderate, and the liberal.

Conservative or Pessimistic Position

This position assumes the worst, that both TCPHDR and IPHDR are maximum that is 60 octet each.

MSS = MTU-60-60 = MTU-120

If MTU is 576 then MSS is 456.

Moderate Position

This position assumes that IPHDR is maximum size (60 octet) and TCPHDR is minimum size (20 octet).

MSS = MTU-60-20 = MTU-80

If MTU is 576 then MSS is 496.

Liberal or Optimistic Position

This position assumes that both the IPHDR and TCPHDR are minimum size, that is 20 octet each.

MSS = MTU-20-20 = MTU-40

If MTU is 576 then MSS is 536.

Default MTU is 576 thus Default MSS is 536. A practical point is raised in favor of the liberal position because percentage of data passed in liberal view is largest.

Experimental Setup

Our research work is simulated on Qualnet 5.2 Simulator. Three Network Parameters namely End to End Delay, Jitter and Throughput, are evaluated under two cases, one in presence of Malicious Nodes and other in absence of it. Table II describes the setting up of Qualnet 5.2 parameters.

We have taken a congested network of 100 nodes and 28 Source-Destination pairs. MSS is varied at the intermediate nodes for packet deformation. The Simulation scenario is given in Figure 1.

Data Analysis

Three network parameters are considered namely End to End Delay, Jitter, and Throughput.

Throughput

Throughput is the average rate of successful data packets received at destination. It is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second.[10]

Table 1. Parameters for Simulation Setup

Parameters	**Value**
Number of Nodes	100
Number of Malicious Nodes	10
Area	1500 m $\times$ 1500 m
Mobility Model	Random Waypoint
Routing Protocol	AODV
Fading Model	None
Shadowing Model	Constant
Reflection Model	Two Ray Ground
Data Rate	2 Mbps
Node Placement	Random Node Placement
Simulation Time	150 Seconds
Channel Frequency	2.4 GHz
Transmission Power	15 dBm
Receiving Sensitivity	-91.0 dBm
Antenna Model	Omni Directional
Traffic Source	CBR
Number of CBR Connection	28
Maximum Segment Size	512, 1024, 2048, 4096

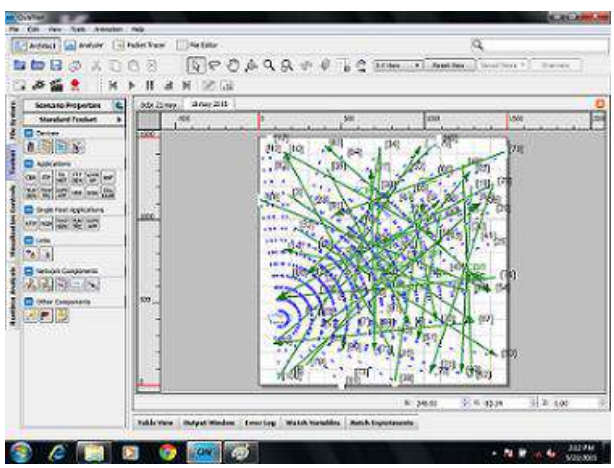

Figure 1. Scenario

End-to-End Delay

Calculating the difference between send times and received times for a specific packet transmitted from source to destination is End to End Delay.[10]

Jitter

Average Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes.[11]

We have taken 28 Source Destination pairs and tried to construct a congested Network with 100 nodes. Two cases are considered, presence of Malicious Nodes represents Case I, and absence of Malicious Nodes represents Case II. Variation in Network performance was observed when 10 Nodes were made Malicious in Case I. We were not able to observe any deformity when Network was not congested. The results of three parameters at few nodes are displayed in the table given below. Table II describes the comparison of End to End Delay, Table III describes the comparison of Jitter, and Table IV describes the comparison of Throughput.

Table 2. End to End Delay

Cases/ Nodes	**10**	**29**	**51**	**69**	**89**
Case I	0.4619	0.6746	2.2301	1.0978	0.3461
Case II	0.9885	0.6769	0.4939	0.6175	0.2670

Table 3. Jitter

Malicious Behavior/ Nodes	**10**	**29**	**51**	**69**	**89**
Case I	0.4619	0.6746	2.2301	1.0978	0.3461
Case II	0.9885	0.6769	0.4939	0.6175	0.2670

Table 4. Throughput

Malicious Behavior/ Nodes	**10**	**29**	**51**	**69**	**89**
Case I	1769	3426	231	2206	330
Case II	3678	2153	291	282	3402

We have considered few nodes to encounter variation in network performance in above Tables. Overview of overall network performance will provide a clear picture. Table V below presents Average Throughput, Jitter and End To End Delay for Case I and Case II.

Table 5. Overall Network Performance

Network Performance / Cases	**Case I**	**Case II**
End To End Delay (s)	0.96633	0.69326
Jitter (s)	0.76783	0.53235
Throughput (bps)	1408.154	1773.38

Figures below demonstrate the change in three parameters namely End to End Delay, Jitter and Throughput. Figure 2 show End to End Delay comparison, Figure 3 shows Jitter Comparison and Figure 4 shows Throughput Comparison.

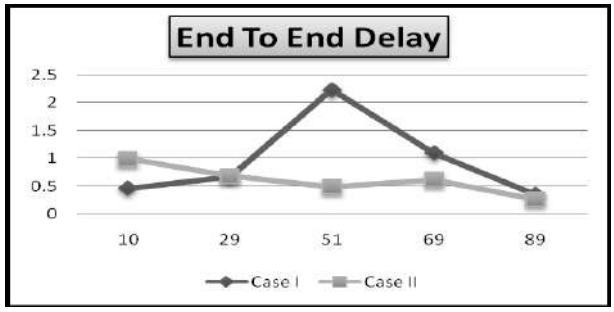

Figure 2. End To End Delay

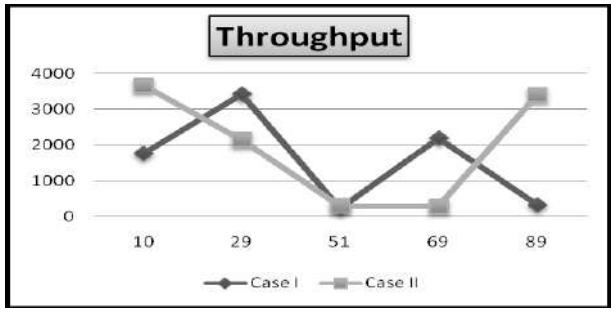

Figure 3. Jitter

Variation differs for nodes, because of traffic flow at the particular node and presence of Malicious Nodes in its surrounding. Variation in MSS at intermediate nodes causes Fragmentation and Reassembly, this changes Network Performance.

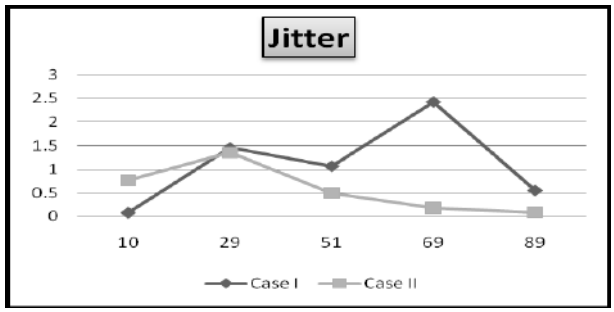

Figure 4. Throughput

Conclusion

This paper has introduced an attack on MANET by varying Maximum Segment size at intermediate node in congested network. This varying of MSS changed Network performance by deforming the packet internally as variation in MSS enabled Fragmentation and Reassembly of packets. This created an extra overhead on Network, this overhead changed Network Parameters.

End to End Delay increases as packets are segmented and assembled because of varying Maximum Segment Size, which causes an extra overhead. Fragmentation hinders Throughput and Defragmentation is a correction to this, thus variation in Throughput. Jitter occurs because of congestion in network. Because of Fragmentation packets get queued and delayed somewhere, thus varied Jitter is received.

References

[1] Basabaa A, Sheltami T and Shakshuki E. Implementation of a3acks intrusion detection system under various mobility speeds. In *5th International Conference on Ambient Systems, Networks and technologies (Ant-2014)*. pp. 571–578.

[2] Al-Roubaiey A, Sheltami T, Mahmoud A et al. Aack: Adaptive acknowledgement intrusion detection for manet with node detection enhancement. In *24th IEEE International Conference on Advanced Information Networking and Applications*. pp. 634–640.

[3] Gagandeep, Aashima and Kumar P. Analysis of different security attacks in manets on protocol stack a-review. *International Journal of Engineering and Advanced Technology* 2012; I(5): 269–275.

[4] Goyal P, Parmar V and Rishi R. Manet: Vulnerabilities, challenges, attacks, application. *International Journal of computational Engineering and Management* 2011; 11.

[5] Saxena T and Deb N. Analytical study of attacks on manets based on layered architecture. *Cyber Times International Journal of Technology and Management* 2013; 6(1): 66–72.

[6] Balakrishnan K, Deng J and Varshney PK. Twoack: Preventing selfishness in mobile adhoc networks, 2005.

[7] Rfc 6691. https://tools.ietf.org/html/rfc6691.

[8] Cs425 lecture 15. http://www.cse.iitk.ac.in/users/dheeraj/cs425/lec15.html.

[9] Path mtu discovery. http://en.wikipedia.org/wiki/Path_MTU_Discovery.

[10] Manju, Thalore R, Jyoti et al. Performance evaluation of bellman-ford, aodv, dsr and dymo protocols using qualnet in 1000m×1000m terrain area. *International Journal of Soft Computing and Engineering* 2013; 2(6).

[11] Sathish S, Thangavel K and Boopathi S. Performance analysis of dsr, aodv, fsr and zrp routing protocols in manet. *MES Journal of Technology and Management* ; : 57–61.