Malicious Attack on MANET using Maximum Segment Size

Laxmi Dike
Computer Science and Engineering Department
Madhav Institute of Technology and Science, Gwalior, India
laxmi.dike87@gmail.com

Abhilash Sonker
Computer Science and Engineering Department
Madhav Institute of Technology and Science, Gwalior, India
abhilashsonkerit@gmail.com

***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.

I. 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 [7,8]. 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.

II. 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. [9,10,11].

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]

DOI-10.18486/ijcsnt.2015.4.10.3
ISSN-2053-6283

III. 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" [1]. 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 [2]:

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"[3]. On receipt of the MSS option the calculation of the size of segment that can be sent is: [2]

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

There are three reasonable positions to take [2]: the conservative, the moderate, and the liberal.

A. 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.

B. 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.

C. 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.

IV. 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.

TABLE 1. PARAMETERS FOR SIMULATION SETUP

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

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.

DOI-10.18486/ijcsnt.2015.4.10.3
ISSN-2053-6283

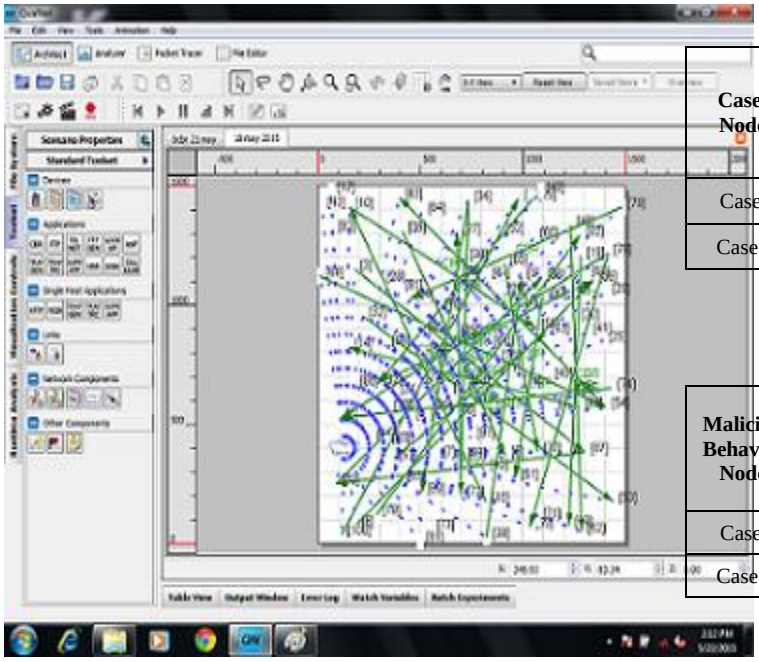

Fig. 1. Scenario

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	0.267

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	0.267

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

V. Data Analysis

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

A. 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. [5]

B. 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. [5]

C. Jitter

Average Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. [4]

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.

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.

DOI-10.18486/ijcsnt.2015.4.10.3
ISSN-2053-6283

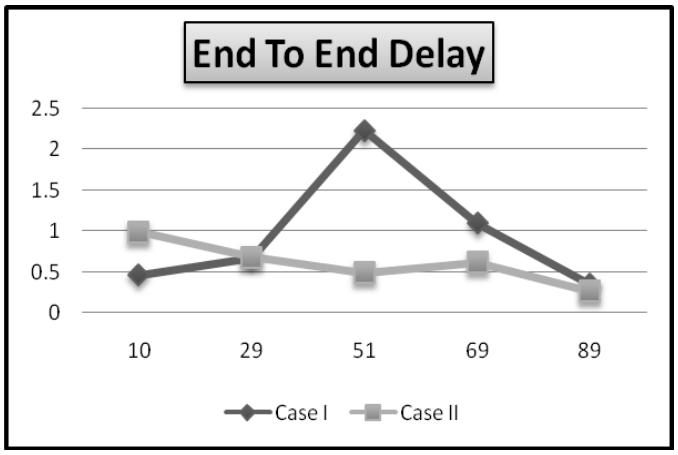

Fig. 2. End To End Delay

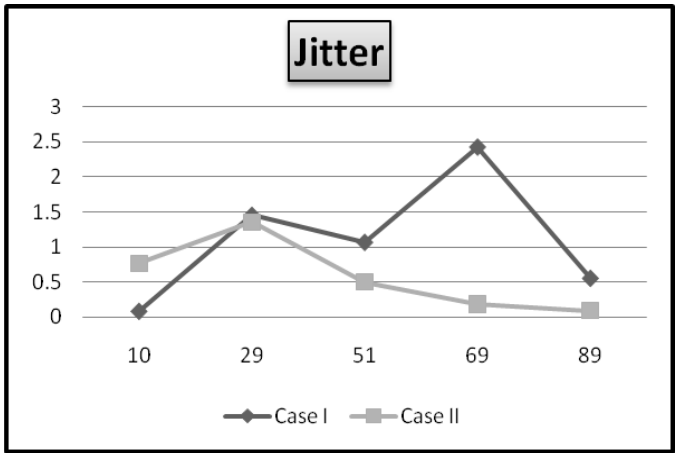

Fig. 3. Jitter

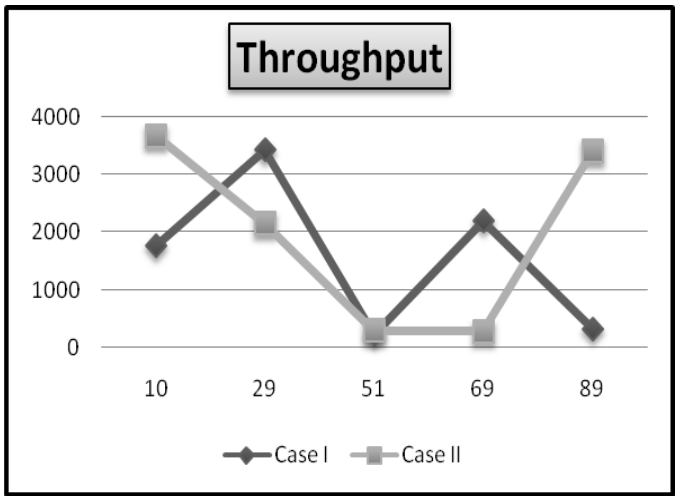

Fig. 4. Throughput

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.

VI. 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] https://tools.ietf.org/html/rfc6691.

[2] http://www.cse.iitk.ac.in/users/dheeraj/cs425/lec15.html.

[3] http://en.wikipedia.org/wiki/Path_MTU_Discovery.

[4] S. Sathish, K. Thangavel and S. Boopathi, "Performance Analysis of DSR, AODV, FSR and ZRP Routing Protocols in MANET", MES Journal of Technology and Management, pp. 57-61.

[5] Manju, R. Thalore, Jyoti and M.K Jha, "Performance Evaluation of Bellman-Ford, AODV, DSR and DYMO Protocols using QualNet in 1000m×1000m Terrain Area ", International Journal of Soft Computing and Engineering, Volume-2, Issue-6, January 2013.

[6] K. Balakrishnan, J. Deng and P. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Adhoc Networks", IEEE 2005.

[7] A. Basabaa, T. Sheltami and E. Shakshuki, "Implementation of A3Acks intrusion detection system under various mobility speeds", 5th International Conference on Ambient Systems, Networks and technologies (Ant-2014), pp. 571-578.

[8] A Al-Roubaiey, T, Sheltami, A. Mahmoud, E. Shakshuki and H. Moutfah, "AACK:Adaptive Acknowledgement Intrusion Detection for MANET with Node Detection Enhancement", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 634-640.

[9] Gagandeep, Aashima and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering

DOI-10.18486/ijcsnt.2015.4.10.3
ISSN-2053-6283

and Advanced Technology, Volume-I, Issue-5, June 2012, pp. 269-275.

[10] P. Goyal, V. Parmar and R. Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", International Journal of computational Engineering and Management, Vol. 11, January 2011.

[11] T. Saxena and N. Deb, "Analytical Study of Attachks on MANETs Based on Layered Architecture", Cyber Times International Journal of Technology and Management, Vol. 6, Issue 1, October 2012-March 2013, pp. 66-72.

Author's Biography

Laxmi Dike is a M.Tech scholar in Computer Science and Engineering Department at Madhav Institute of Technology and Science, Gwalior, India. She received her Bachelor degree (B.E.) in Computer Science and Engineering from Jabalpur Engineering College, Jabalpur in 2009. Her area of research is Mobile Ad hoc networking, Wireless Network.

Abhilash Sonker, received his Bachelor degree (B.E.) from SATI, Vidisha in 2006, Master degree (M.Tech) from MANIT, Bhopal in 2009. He is currently Assistant Professor in Information Technology Department at Madhav Institute of Technology & Science, Gwalior, India. His current research interests include Mobile Adhoc Network and Network Security.

DOI-10.18486/ijcsnt.2015.4.10.3
ISSN-2053-6283