

Performance Improvement of Mobile Ad hoc Networks under Jamming Attack

Snehita Modi¹, Dr. Paramjeet Singh², Dr. Shaveta Rani³

^{1,2,3}Computer Science Department, Punjab Technical University
Giani Zail Singh University Campus, Bathinda, India

Abstract: A collection of mobile nodes having ability to organize in a free manner without any fixed infrastructure is known as Mobile Ad hoc Networks (MANETs). Among various types of wireless networks, MANETs are one of the most usable network types. Various routing protocols are there to route the optimal path in an ad hoc network. But because of the wireless nature of MANETs, security of networks is a major issue. It is prone to various types of malicious attacks. Jamming attacks are one of them. These occur by transmitting continuous radio waves to inhibit the transmission among sender and receiver. These attacks effect the network by decreasing the network performance. Previously there had been considerable research in the field of increasing the performance of network by using routing protocols. In our research work we are improving the performance of mobile ad hoc networks under jamming attack by using an integrated approach. The proposed work includes a network with high mobility, using IEEE 802.11g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high data rate are being generated in the network. The performance of network is measured with respect to the QoS parameters like throughput, retransmission attempts, network load and media access delay. OPNET (Optimized Network Engineering Tool) MODELER 14.5 is used for simulation. The results of simulation demonstrate that the overall performance of network with jamming attack has been increased by using the integrated approach.

Keywords: MANETs, Jamming Attack, Throughput, Retransmission attempts, OPNET.

I. INTRODUCTION

Mobile Ad hoc Networks have been in use for a long period. A mobile ad hoc network (MANET) is a network of wireless mobile nodes which co-operate to maintain network connectivity and exchange information [1]. MANETs are very useful in cases where wired network installation is infeasible such as battlefields and buildings with no previous network cabling [1]. Because of the absence of any centralized control or access point, MANETs has self-configuring nature. The nodes have the ability to move randomly and organize them in an arbitrary manner [1]. Due to this routing protocols are required to establish routes among the mobile nodes. There are mainly two types of routing protocols in MANETs. These are reactive and proactive routing protocols. In a network configured to use reactive routing protocols, routes are established from source node to destination node when required by the application or when there is some data to be exchanged between the nodes [2]. Apart from the choice of routing protocol, nodes present in the network (node

density) and their level of mobility (node mobility) also affect the performance of the network [2].

The absence of fixed infrastructure of MANETs makes it more prone to threats; hence security is a key issue. Different malicious attacks are there out of which Jamming attack is very common.

In this paper, we have analyzed and improved the performance of mobile ad hoc network routing protocol under jamming attacks by using network with high mobility nodes [2], IEEE 802.11g standard [4][9] with a data rate of 54mbps along with improved AODV routing protocol [5].

II. JAMMING ATTACK

The most popular attack model of IEEE 802.11 is Jamming Attacks [3]. As compared to wired networks, ad hoc networks are more prone to security threats. Jamming attack is one of the types of Denial of Service (DoS) attack. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets on the network [3].

Various adversaries are responsible for the jamming attack. These adversaries aim at prohibiting the sender/receiver transmission. Jamming is caused by continuously sending the radio signals in between the transmission which injects the dummy packets thus causing interferences. As radio frequency is an open medium, hence for wireless networks jamming is a big problem. Jamming decreases the performance of network by effecting its throughput, network load, end to end delay etc.

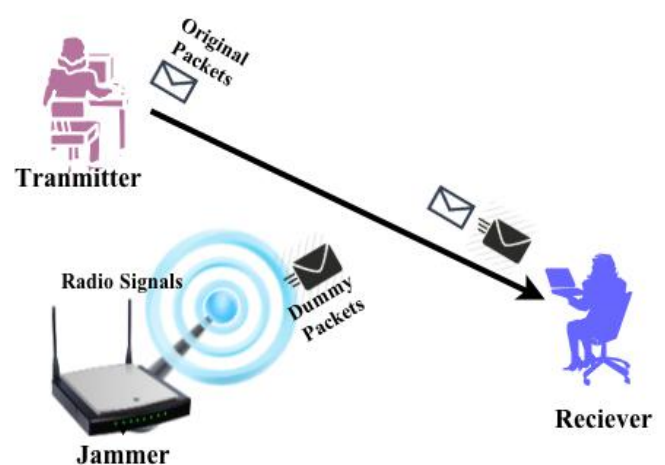


Fig. 1 Jamming Attack

III. RELATED WORK

Thriveni H.B., G. Manoj Kumar, Rinki Sharma [2] analyzed the performance of mobile ad hoc networks with varying node mobility and node density. They selected DSDV and DSR routing protocols. The network performance was measured in terms of various parameters. They came to a result that DSR protocol outperforms DSDV if the network mobility and node density s varied.

Arif Sari, Dr.Beran Necat [3] used unified security mechanism in order to improve the network performance. They used a combination of PCF (Pont Control function) and RTS CTS mechanism. OPNET simulation tool was used for entire network performance.

Rohit Sharma [4] developed simulator to simulate the behavior of various standards of wireless network. "Simabg" Simulator was the proposed wireless system designed to analyze and compare different routing physical standards of IEEE 802.11 (IEEE 802.11b, IEEE 802.11a and IEEE 802.11g) on certain parameters such as Media Access Delay, Network Throughput, Network Bandwidth Utilization and Total Packet Delay.

Firat Tekiner, Ashish Shrestha [5] focused on investigation of the performance of reactive and proactive MANET routing protocols, namely AODV, DSR, TORA and OLSR. The performance of networks was computed varying in sizes by increasing area and nodes size to investigate mobility and scalability of the routing process. The protocols were tested using the same parameters with high CBR traffic flow and random mobility.

Agustin Zaballos, Alex Vallejo, Guiomar Corral, Jaume Abella [6] demonstrated that proactive protocols introduce a lower delay in the network. Different scenario situations were considered here for various routing protocols.

IV. METHODOLOGY

This section describes the simulation tool used along with the proposed method.

A. Simulation tool used:

OPNET modeler (v14.5) is extensive and a very powerful simulation software with wide variety of possibilities. The entire heterogeneous networks with various routing protocols can be simulated using OPNET. High level of user interface is used in OPNET which is constructed from C and C++ source code blocks.

B. Simulation Setup:

The simulation focuses on improving the performance of MANETs under jamming attack. Therefor an Integrated approach is used to improve the network performance under jamming attack. This approach includes:

- Network with high mobility [2]
- High data rate of 54mbps by using IEEE 802.11g standard [9]
- Improved parameter of AODV routing protocol
- Generation of high resolution video conferencing and FTP traffic

1) Profile Configuration Parameters:

The "Profile Config" node can be used to create user profiles. These profiles are then specified on different nodes in the network to generate application layer traffic. Here FTP traffic start time is taken as constant 55 and Video conferencing start time is taken as constant 75.

2) Application Configuration Parameters:

The traffic used is FTP traffic and video conferencing of high resolution.

3) Routing Protocol Parameters:

AODV routing protocol is applied on all the nodes with a change in parameters. In scenario with integrated approach, the "hello" interval time of AODV parameter is increased from the default value to decrease the congestion in the topology [7].

TABLE 1
AODV PARAMETERS

Active route timeout (seconds)	30
Hello Interval (seconds)	Uniform(10,10.1)
Allowed Hello Loss	10
Timeout Buffer	2
Addressing Mode	IPv4

4) RX configuration Parameters:

These are receiver transmitter configuration parameters. The refresh time for node is set to every 10 seconds and for remaining parameters the default setting is chosen for the RX configuration in the network.

TABLE 2
RX CONFIGURATION PARAMETERS

Begin Time (seconds)	Start of Simulation
End Time (seconds)	End of Simulation
Refresh Interval (seconds)	10

5) Mobility Configuration parameters:

This node controls the movement of nodes based on the configured parameters. Random waypoint model of mobility is used with vector trajectory.

6) Wireless Parameters:

The wireless LAN parameters configured have been taken from the research work of [27], except the size of buffer. Because of heavy data flow of the chosen application traffics, the buffer size is increased to 102400000. The data rate has been chosen maximum of 54 bits by using IEEE 802.11g standard. In addition, the channel settings were set to "auto assigned" in order to avoid manual error. The transmission power is increased from 0.005 watt to 0.030 watt.

TABLE 3
WIRELESS LAN PARAMETERS

Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	54 mbps
Transmit Power (W)	0.030
Packet Reception-Power Threshold	-95
Rts Threshold (bytes)	None
Short Retry Limit	7
Long Retry Limit	4
Buffer Size	102400000

7) *DES configuration Parameters:*

The total time taken for DES simulation was 600 seconds (10 mins). Every scenario has been run for the same time.

TABLE 4
DES PARAMETERS

Duration	600 seconds
Seed	128
Values per static	100
Update interval	500000 events

Three scenarios have been created with 30 nodes each. One scenario is with AODV routing protocol with no jamming attack, another is with AODV and jamming attack, third and the last scenario is with integrated approach for improving network performance.

8) *Jammer parameters:*

Pulse width jammer is taken causing the jamming attack.

TABLE 5
JAMMER PARAMETERS

Name	Jammer
Trajectory	VECTOR
Jammer band base frequency	2,402
Jammer Bandwidth	100,000
Jammer Transmitter Power	0.001
Pulse width	1.0

9) *QoS Parameters:*

Global QoS parameters have been taken for MANET as well as Wireless networks. These are delay, throughput, network load and retransmission attempts.

TABLE 6
QOS PARAMETERS

Media Access Delay
Retransmission Attempts
Network Load
Throughput

V. RESULTS AND GRAPHS

A. *Media Access Delay:*

It is the duration in sending the media packet and the receiving of that packet at receiver end.

It is shown in the figure 2 that media access delay is highest with jamming attack which is decreased by applying the proposed mechanism. It is because of the increased buffer size.

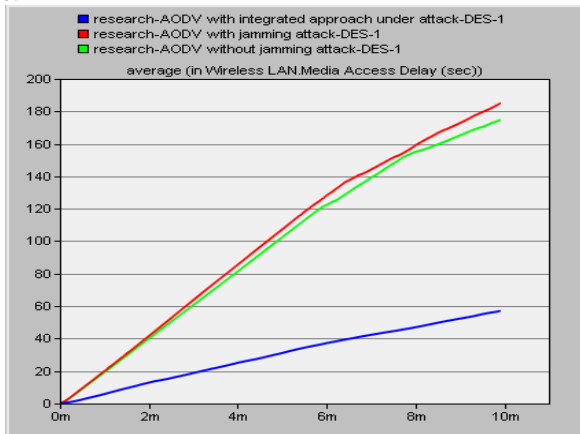


Fig 2 Average Media Access Delay

B. *Retransmission attempts:*

The number of retransmission attempts by all WLAN MACs in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.

Figure 3 shows that network with jamming attack has less attempts but the integrated approach increases the retransmission attempts to a great extent. It happens due to the increased “Hello” packets of AODV routing protocol.

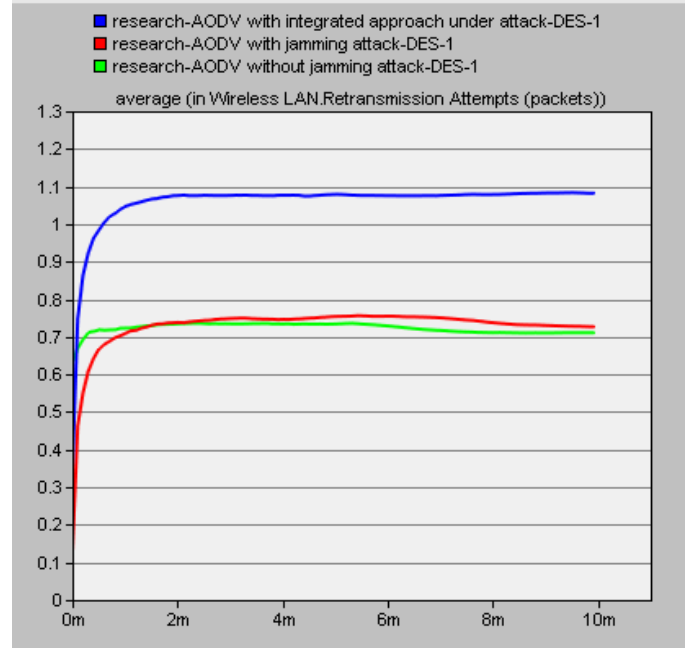


Fig. 3 Average Retransmission Attempts

C. *Network Load:*

Network load is increased by the proposed mechanism which is due to the high data traffics and high data rate.

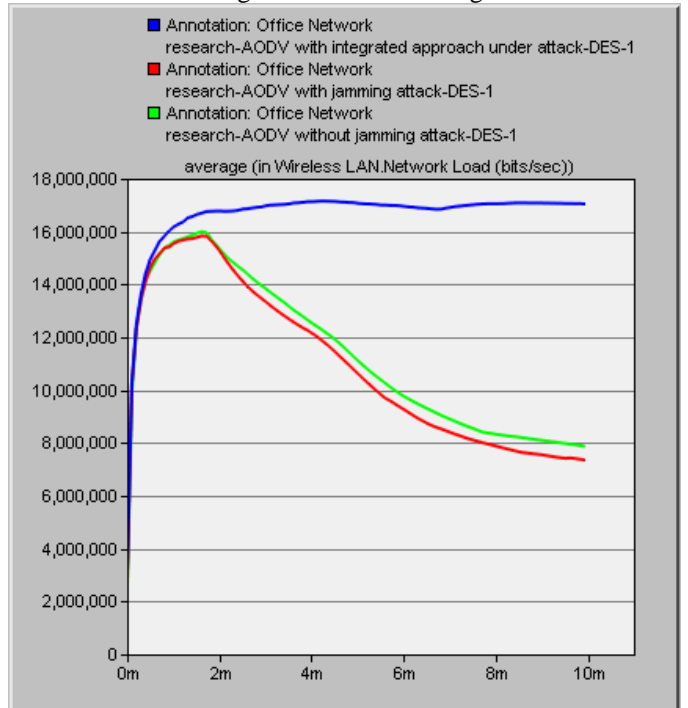


Fig. 4 Average Network Load (bits/sec)

D. Throughput (bits/sec):

It is the number of packets received by all the destinations over the duration of simulation [9]. The network with jamming attack and misbehaving nodes decreased the throughput as shown in figure 4 however the throughput of entire network is increased remarkably when the proposed mechanism is applied. In scenario with AODV and integrated approach, 11,000,000 packets are received which goes on increasing with respect to time and reaches to 15,000,000 approx. because of high data rate of 54 mbps AODV outperforms.

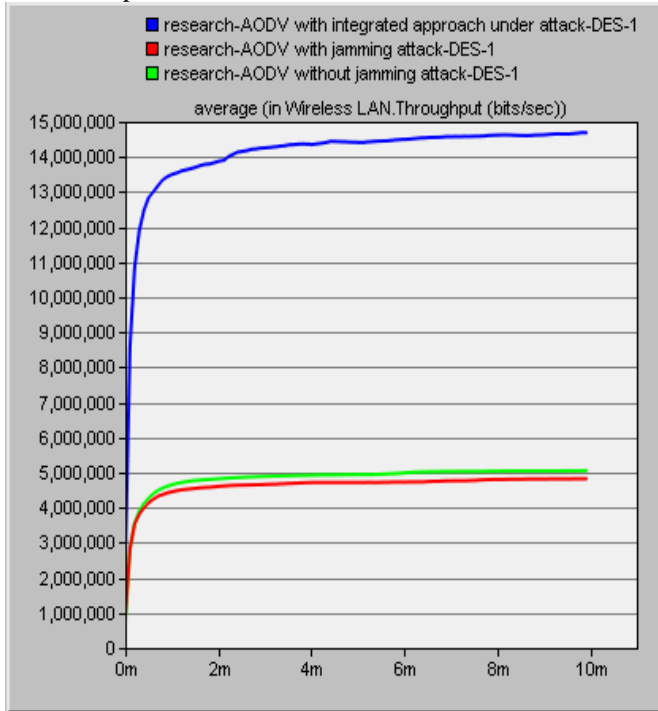


Fig. 5 Average Throughput (bits/sec)

VI. CONCLUSION

Because of the wireless nature of mobile ad hoc networks, various attacks are performed to degrade the network performance. Jamming attack is one of them. Therefore routing protocols are used to increase the network throughput. In this research work, the network performance under jamming attack is improved by applying integrated approach. This approach includes a network with high mobility, IEEE 802.11g standard with max data rate, heavy

traffic like FTP and video conferencing, improved AODV parameters and increased buffer size. In our paper, it was shown that jamming attack reduces the network throughput, retransmission attempts and increases the media access delay. By applying the proposed mechanism, the network throughput increases drastically, also there is an increase in retransmission attempts and the media access delay decreases. The overall performance of network increases except the network load which is increased by the proposed mechanism. Hence, in future some addition to this proposed work is to be done to decrease the network load.

REFERENCES

- [1] Ashish Bagwari (IEEE member), Raman Jee, Pankaj Joshi, Sourabh Bisht, "Performance of AODV Routing Protocol with increasing the MANET Nodes and it's effects on QoS of Mobile Ad hoc Networks" 2012 International Conference on communication Systems and Network Technologies, pp 320-324, May 2012, ISBN: 978-1-4673-1538-8 .
- [2] Thriveni H.B., Manoj Kumar, Rinki Sharma, "Performance Evaluation of Routing Protocols in Mobile Ad-Hoc Networks with Varying Node Density and Node Mobility", IEEE 2013 International Conference on Communication Systems and Network Technologies, pp 252-256, April 2013, ISBN: 978-0-7695-4958-3.
- [3] Arif Sari, Dr. Beran Necat, "Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.3, No.3, June 2012, pp 79-94.
- [4] Rohit Sharma, "Simulator to Analyze QoS for IEEE 802.11b/a/g standards", IJCSIT, Volume 1, Issue 2, December 2010, pp 91-96.
- [5] Ashish Shrestha, Firat Tekinar, "On MANET Routing Protocols for Mobility and Scalability", IEEE International Conference of Parallel and Distributed Computing, Applications and Technologies, pp 451-456, December 2009, ISBN: 978-0-7695-3914-0.
- [6] Agustín Zaballos, Alex Vallejo, Guiomar Corral, Jaume Abella, "AdHoc routing performance study using OPNET Modeler", OPNETWORK '2006, Washington DC (United States), pp 1-6.
- [7] Qasim Nadia, Said Fatin & Aghvami Hamid, "Mobile Ad Hoc Networking Protocol's Evaluation through Simulation for Quality of Service", IAENG International Journal of Computer Science, 36:1, IJCS_36_1_10, February 2009.
- [8] Harmanpreet kaur, Er. Jswinder Singh, "Performance comparison of OLSR, GRP and TORA using OPNET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012, pp-260-267.
- [9] Anjali, Maninder Singh, "Simulation and Performance Analysis of AODV, OLSR, GRP Routing Protocol by considering IEEE 802.11Standard", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 6, June 2012, pp-171-178.
- [10] OPNET modeler 14.5. <http://www.opnet.com/solutions/networkrd/modeler.html>.