ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Mitigation of Jamming Attack in Mobile Ad Hoc Networks

Pawani Popli[1], Paru Raj[2]

M.Tech Student, Department of CSE & Prannath Parnami Institute of Management & Technology, Hisar, Haryana, India [1]

Asst. Professor, Department of CSE & Prannath Parnami Institute of Management & Technology, Hisar, Haryana, India[2]

ABSTRACT: Due to the wireless behaviour of the channel and specific characteristics of MANETs, the radio disturbance attacks cannot be eliminated by conventional security mechanisms. An antagonist can easily dominate over its medium access control protocol (MAC) and seamlessly transmit packages on the network medium. The authenticated nodes hold propagating Request-to- Send (RTS) frames to the access point node for accessing the shared channel and start data transfer. Since, due to jamming attacks on the network, the access point node cannot assign authentic access to shared medium. These attacks lead significant decrement on whole network packet transmission rates, delay and throughput on the MAC layer however other nodes pull out from the interaction. The proposed technique used for mitigating and preventing jamming attacks is enforced at the MAC layer that has an integration of several coordination techniques. These are an integration of Point Controller Functions (PCF) that are used to coordinate entire network activities at the MAC layer and RTS/CTS (Clear-To-Send) mechanisms which is a handshaking procedure that decreases the collisions on the wireless network. The entire network performance and technique is simulated by using OPNET modeler.

KEYWORDS: MANET, PCF, OPNET Simulation, RTS/CTS, Unified Security mechanism, Jamming Attack.

I. INTRODUCTION

A MANET stands for Mobile ad hoc Network. It is a set of mobile nodes that interact over relative bandwidth restrained wireless links. The network configuration unpredictably and frequently changes over time due to nodes mobility. The network is not centralized such as decentralized, where all network activity involving delivering messages and finding the configuration all must be executed by the nodes themselves, i.e., routing service will be contained into mobile nodes. To find the network topology, routing and link scheduling require distributed algorithms, irrespective of applications. The group of applications is ranging for small scale, mobile, diverse, highly dynamic networks, stationary networks that are restrained by power to large scale. In decentralized atmosphere determining feasible routing paths and delivering messages is not a well-explained problem where network configuration changes. In stationary network often utilize the optimum route to determine the shortest path from source to destination node but this concept is not easily explored to MANETS. The network should be capable to change the routing paths to the factors i.e. propagation path loss, fading, variable wireless connection quality, multiuser interferences, topological changes, power expended. This is a complicated issue to design a network protocol for this network. Still, MANET reliability builds an interesting option to conventional networks structures.

II. JAMMING ATTACK

In starting, in jamming attack intruder keeps scanning on wireless media and also examine the frequency at which target node achieving the signals from the sender. Signal is transferred on that frequency to hinder error free receptor.
The primary objective of jammer is to attempting to obtain the reception of wireless interactions with the physical transmission. A jammer always attempt to achieve the legal traffic will totally blocked by constantly transmits RF signals to fill a wireless medium. In this attack jam the transmission channels no. of source are built rather than single source which forwards crude packets to the transmission channels and jammed the channel. Due to jamming, packet

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

loss begins. It reduces the reliability and efficiency of the system. Several problems arise because of this attack i.e. delay in transmission, channel becomes busy, new packets being dropped etc. Jamming attacks are primarily classified into two kinds: Physical and Virtual Jamming. Physical or Radio jamming takes place by seamless emission of radio signals or by forwarding random bits onto the channel and/or at the recipient by causing packet collisions. Virtual jamming can take place at the MAC layer through attack on RTS/CTS frames.

III. RTS/CTS MECHANISM

One of the main causes for utilizing the RTS/CTS technique is to avoid network level congestion and also prevent and protect the network from hidden jammer node attacks issue from the network perspective. In infrastructure-based networks RTS/CTS technique normally works well, in some circumstances it may yield to unfairness. Since, in general establishing ad hoc networks, the RTS/CTS technique provides rise to situation where huge no. of nodes is not able to transfer any packet. These can yields to network-level congestion conditions. The Request to Send/Clear to Send (RTS/CTS) technique is a handshaking procedure when hidden nodes are working on the network that decreases the happening of collisions. Working of RTS/CTS technique implementation is explained in Fig below.

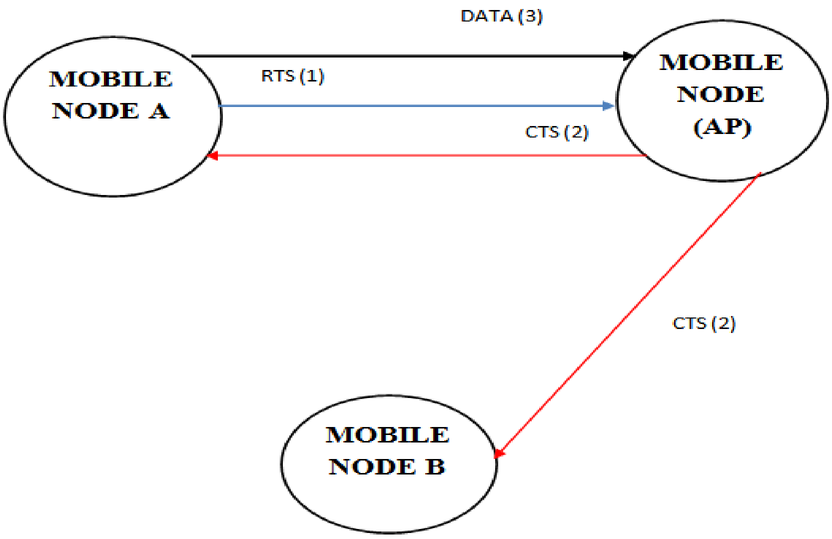

Figure 1: AP mobile node receives RTS data from Mobile node

When mobile node A wish to forward a packet to mobile node AP it initially forward a small packet known as RTS (Request-To-Send) and responses to it with small packet CTS (Clear-To-Send). After obtaining CTS , node *A* forwards the *DATA* packet to node *AP*. In-between mobile node B obtains the CTS packet however the Mobile Node A is forwarding data and the technique reports the mobile Node B that the AP is transferring or obtaining data at that time frame and Mobile Node B to wait for a specific time. Fake RTS frames are forwarded to the AP mobile node When a jamming attack is established on the network, that holds the medium busy or proposes packet collisions causing forced and prevents other nodes from being capable to start with legitimate MAC operations, and repeated back offs.

3.1 RCCA Algorithm

Assume the network configuration with four nodes which are in the transmission coverage range of one another. Here the probability of RTS/CTS collision cannot be ignored. The introduced algorithm, attempts to decrease the probability of selfish nature occur in the CW.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Frame Control	Duration	Receiver Address	Transmitter Address	Active Neighbour Bit (ANB)	FCS

MAC header

Figure 2: MAC Header

In multihop networks, nodes often utilizes BEB algorithm on collision and utilizes back off counter value to show the no. of back off slots. When back off counter value (BC) arrives zero, nodes begin transferring the packets. In RCCA algorithm, every station forwards a particular packet known as Collision Avoidance Packet (CAP) which has the information about source address, destination address and Active Neighbour Bit (ANB).This packet should be forwarded before two slots in advance. The RCCA algorithm formulated to determine the collisions in two hop neighbours is illustrated in Fig 3. It is viewed that often at BC=0, nodes initiate the interaction. But in this protocol, when the BC value becomes 2, I begin to forward the CAP to the recipient which provides the information about whether any interaction is going on within the transmission coverage range. If

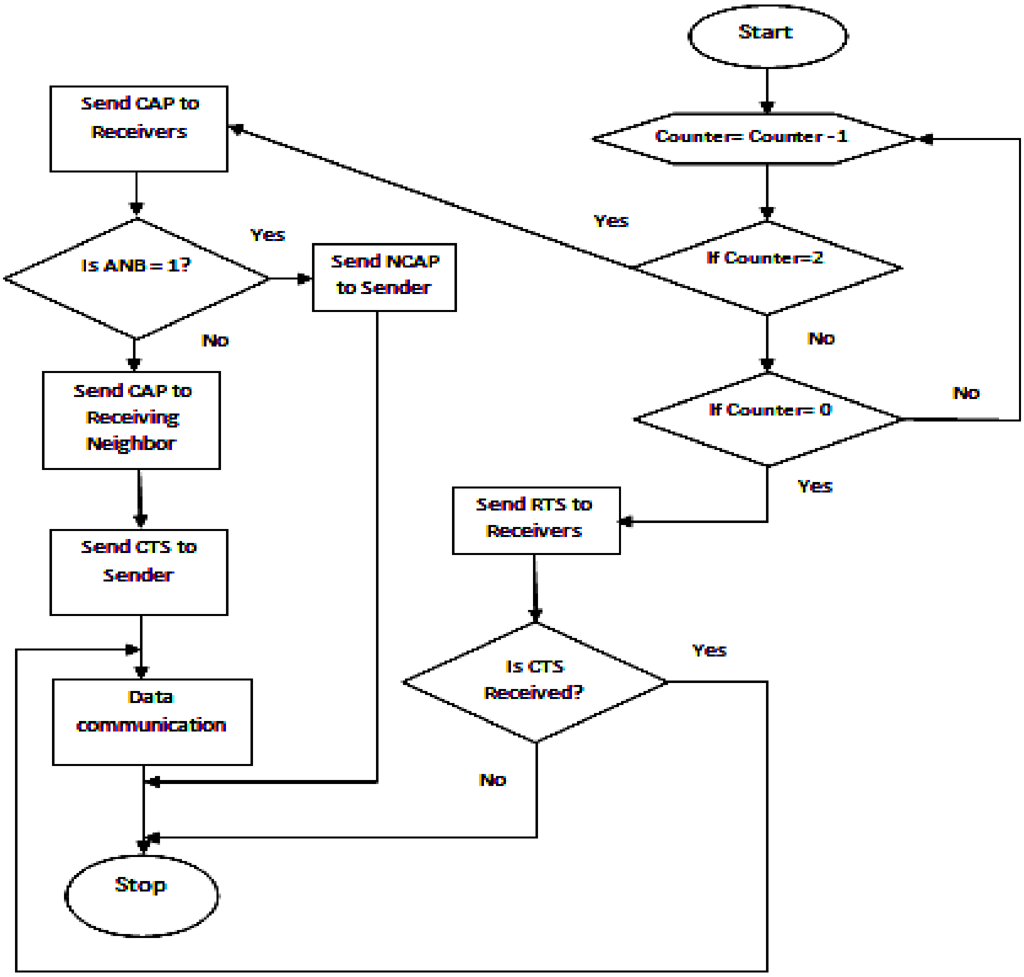

Figure 3: Flowchart of Proposed Modified RTS/CTS mechanism

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

so, then the ANB bit is equal to 1. It forwards a Negative Collision Avoidance Packet (NCAP) to the forwarder to cease the communication. So, the sender will not forward any packet to the recipient till the recipient intimates with a CTS packet. If there is no interaction going on within the transmission coverage range of recipient, ANB is set to zero. Now the recipient forwards the CAP to its neighbouring nodes. After listening the CAP, the neighbouring nodes will not interrupt the recipient till the data transmission completes. Before the back off counter arrives zero, the above interaction should ends. When the back off counter arrives zero, it continues with the basic RTS-CTS handshake mechanism. From the above introduced mechanism collision can be ignored at the recipient side. The selection of small CW value by selfish nodes can be neglected.

IV. RESULTS

After showing all simulations basic results conducted in both scenarios, in this chapter, we examine and explain all these results. The performance metrics gathered and showed in our results are either depends on the global statistics or object statistics of the MANET model such as the whole network. In presenting these data, we showed the results average or time average values in this report. We begin our discussion and analysis with the two significant scenarios in which the first scenario contains 100 mobile nodes and the second scenario contain 200 mobile nodes. In every scenario, we did two simulations of a continuous network operation in MANET and in MANET, a Jamming attack to be precise. All simulations such as both scenarios were operated for a specific time period of 30 minutes, which ranged from 0 to 1800 seconds as presented in the result graphs. After that, we examine and compare within every scenario and also both scenarios depend on their end to end delay and throughput. Basic parameters utilized for experimentation with OPNET modeler. Communication region is 55 x 55 km with 150 and 200 mobile nodes. The comparison of performance of three scenarios with respect to throughput is illustrated in fig. The total simulation performance is explained in nutshell in the following table, which shows that the removal of jamming attack scenario offers the better results and attempt to normalize the jamming influenced network to its normal state as near as possible.

Table 4.1. Simulation Parameters

Simulation Parameters	
Examined Protocols	AODV
Number of Nodes	150, 200
Types of Nodes	Mobile
Simulation Area	55 x55 km
Simulation Time	1800 seconds
Mobility	10 m/s
Pause Time	100 seconds
Performance Parameters	Throughput, Delay
Traffic type	FTP
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Wireless LAN MAC Address	Auto Assigned
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	256
Packet-Reception Threshold	95
Long Retry Limit	4
Max Receive Lifetime(seconds)	0.5
Buffer Size(bits)	256000

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

4.1 Throughput:

Throughput can be explained as the ratio of the total amount of data arrive a destination node from the source node. The time it consumes by the destination node to obtain the last message is known as throughput. It can be represented as bytes or bits per seconds (byte/sec or bit/sec). There are some factors that influence the throughput i.e. existence of restricted bandwidth, changes in topology, unreliable communication among nodes and restricted energy. A high throughput is right choice in each network. In fig the graph shows the throughput in bits/sec. The x-axis presents the simulation time in min and the y-axis shows throughput in bits/sec.

Scenario 1, shows the scenario with no malicious event and normal network state, scenario 2 shows the network that is with the jamming attack and scenario 3 shows the mobile jammers and implementation of the introduced technique. It can be clearly viewed, that the jamming attack reduces the total network throughput as compared to the normal network state. Since, the throughput of whole network is increased once the introduced unified technique is implemented. Additionally, the throughput state has increased more than the no attack scenario after enforcing the unified security technique.

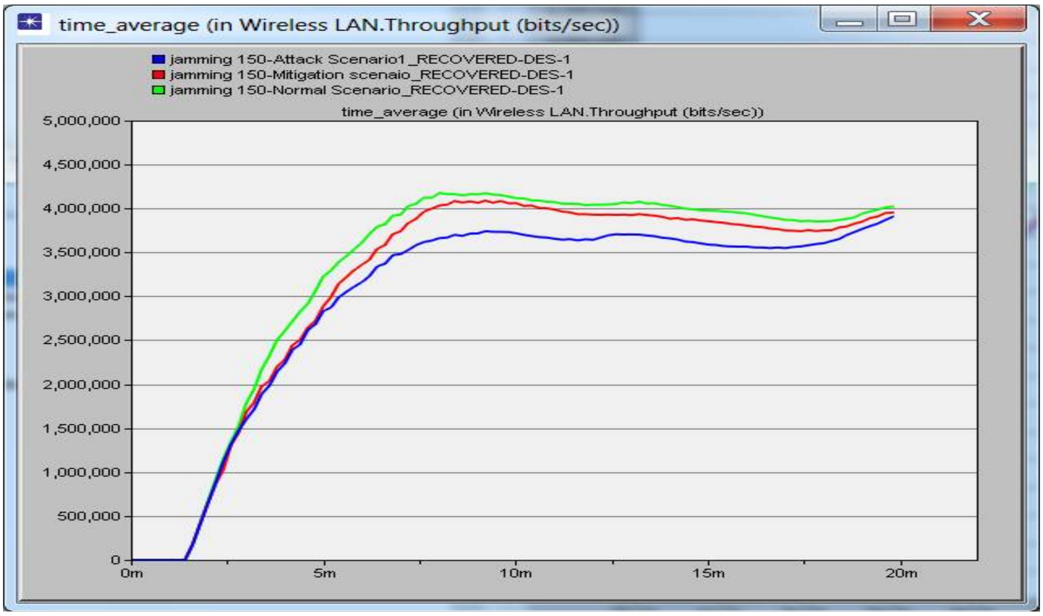

Figure: 4 Throughputs of All Three Scenarios at 100 Nodes

In first scenario of 150 nodes of our experimentation, packets travels are represented as throughput with maximum value of about 3566213 bits/sec and it is shown as bits per second. In second scenario which is under jamming attack, packets drops which are explained as throughput, reduces to value of about 3227315 bits/sec. In first scenario of 200 nodes of our experimentation, packets travels are represented as throughput with maximum value of about 14563478 bits/sec and it is expressed as bits per second. In second scenario which is under Jamming attack, packets drops which are explained as throughput, reduces to value of about 10435675 bits/sec.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

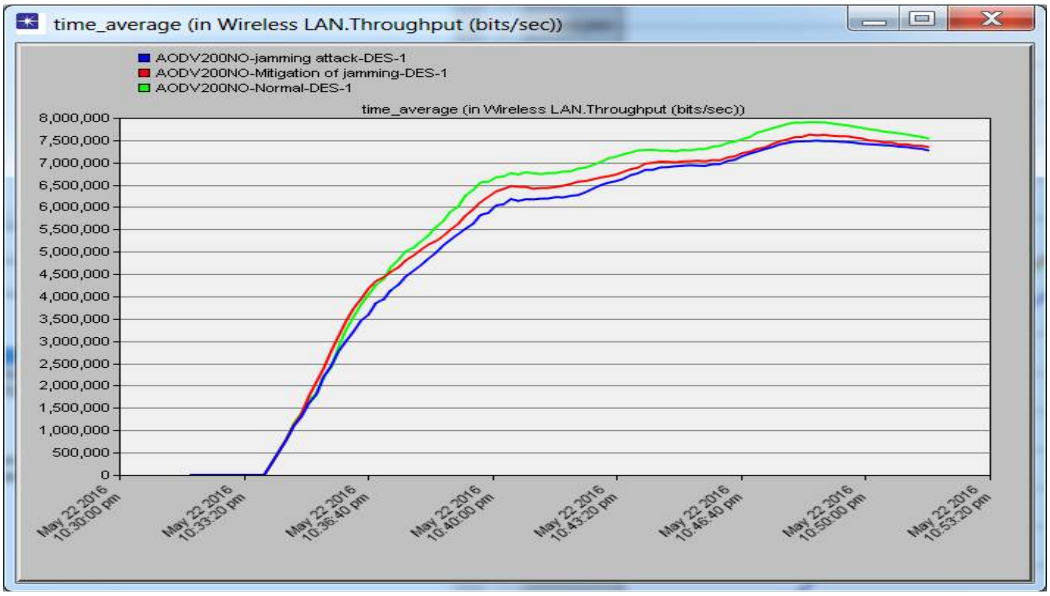

Figure: 5 Throughputs of All Three Scenarios at 200 Nodes

This packets drop in form of throughput is because of the jamming effect. The throughput recovery occurs with introduced technique by removal of the jamming attack as throughput comes same as the normal scenario.

4.2 End To End Delay:

The packet end to end delay is the average time that packets consume for network traversing. This is the time from the packet creation generation by the sender node up to their reception at the target node and is represented in seconds. Thus all the network delays are known as packet end-to-end delay. It involves all the network delays i.e. Processing delay (PD), propagation delay (PD), queuing delay (QD), transmission delay (TD).

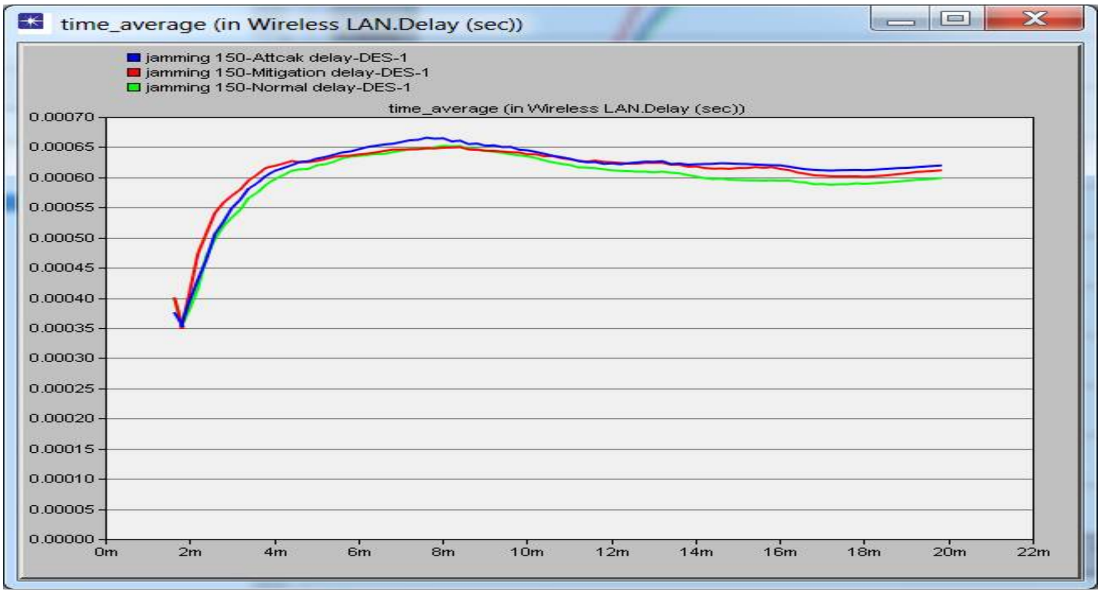

Figure: 6 Delay Of All Three Scenarios at 150 Nodes

In first scenario of 150 nodes of our experimentation, packets Delay are represented as fig 6 with maximum value of about 0.00065 seconds. In second scenario which is under jamming attack, packets delay Increases to value of about

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

0.00072 seconds. In first scenario of 200 nodes of our experimentation, packets delay is about 0.0009 seconds. In second scenario which is under jamming attack, packets delay value increases about 0.0016 seconds.

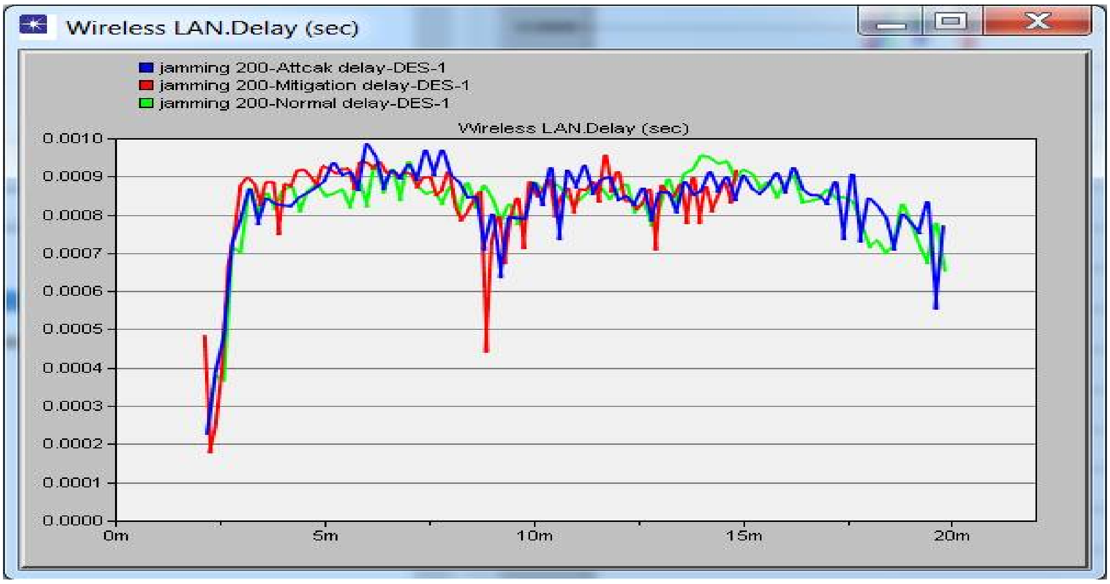

Figure: 5.4 Delay Of All Three Scenarios at 200 Nodes

The end to end delay recovery reduces with our introduced technique by removal of the jamming attack as end to end delay comes same as the value 0.000256 seconds. Hence our introduced techniques remove jamming attack in network.

V. CONCLUSION

Jammers attacks will have an impact on performance of networks as a result of the jammers disrupts with the conventional network operation. The impact of intruders studied in this paper was by increasing delay, data dropped traffic obtained and forwarded and reducing network packet drop ratio. In this research work, the performance of network under jamming attack is examining by using integrated mechanism. The objective of this simulation research study was to realize the effect of an integration of security techniques against jamming attacks. The unified technique is implemented on the chosen nodes on the network and deployed in the particular region. The discovery of the research clearly specifies that, the implementation of such unified techniques have an important effect on the total network through positively. On the other side, the implementation of these techniques does not only mitigate the jamming attack impacts, it also increases the total performance above the network normal state. The unified technique that consist an integration of RTS/CTS and PCF represents adequate performance in MANET. However 2 mobile jammers utilized in this simulation experiment, the introduced security technique satisfactorily mitigated the jamming attack impacts on the network and increased the total network performance while enhancing data drop rate. The data dropped rate reduces successfully. However the jamming attack yields packet drop rate and low throughput effect on the network, the rate of delay appears acceptable on the network. Future studies can be conducted to change the current model to reduce total network delay.

REFERENCES

[1] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar," Improving Reliability of Jamming Attack Detection in Ad-Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 3, No.1, April 2011, pp. 57-66.
[2] S. Raja Ratna, R. Ravi and Dr. Beulah Shekhar," Mitigating Denial of Service Attacks in Wireless Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, No.5, May 2013, pp. 1716-1719.
[3] Sabbar Insaif Jasim," Jamming Attacks Impact On the performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing protocols," International Journal of Engineering and Advanced Technology(IJEAT), Volume 3, Issue 2, Dec. 2013, pp. 325-330.
[4] Ajana J., Helen K.J, "Mitigating Inside Jammers in MANET Using Localized Detection Scheme", International Journal of Engineering Science Invention, Volume 2, Issue 7, July 2013, pp. 13-19.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[5] Snehita Modi, Dr. Paramjeet Singh, Dr. Shaveta Rani," Performance Improvement of Mobile Ad-Hoc Networks under Jamming Attacks" , International Journal of Computer Science and Information Technologies, Vol. 5, 2014, pp. 5197-5200.
[6] Gagandeep, Aashima, Pawan Kumar ,"Analysis Of Different Security Attacks in MANET on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012, pp. 269-275.
[7] Arif Sari and Dr. Beran Necat," Security 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.
[8] P.Ramesh Kumar, G.Nageswara Rao and P.Rambabu," Packet Classification Method to Counter Jamming Attacks in Ad-Hoc Networks", International Journal for Development of Computer Science & Technology, Volume-1, Issue-5, Aug-Sep 2013, pp. 31-36.
[9] Agustin Zaballos, Alex Vallejo, Guiomar Corral and Jaume Abella," AdHoc routing performance study using OPNET Modeler", University Raman Llull Barcelona (Spain), pp. 1-6.
[10] Swati Puri, Vishal Arora," Performance of MANET ", International Journal of Engineering Trends and Technology (IJETT), Volume 9, Number 11, 11 Mar. 2014, pp. 544-549.
[11] Aashish Mangla, Vandana," Prevention of Jamming Attack in MANET ", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015, pp. 2307-2311.
[12] Syeda Arshiya Sultana, Samreen Banu kazi, Parveen Maniyar and M.Azharuddin," A Survey on Selective Jamming Attacks in WMNs", International Journal of Computer Applications Technology and Research, Volume 4, Issue 5, 2015, pp. 380-385.
[13] Aashish Mangla, Vandana," Detection of Physical Jamming Attacks in MANETs", International journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015, pp. 1972-1976.
[14] Upma Goyal, Mansi Gupta, Kiranveer Kaur," Meliorated Detection Mechanism for the detection of Physical jamming Attacks under AODV and DSr protocols in MANETs", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 10, Oct. 2014, pp. 134-144.
[15] Henna Khosla, Rupinder Kaur," Jamming Attack Detection and Isolation to Increase Efficiency of the Network in Mobile Ad-Hoc Network", International Research Journal of Engineering and Technology (IRJET), Volume 2, Issue 4, July 2015, pp. 510-516.
[16] Jaspreet Kaur, Dr. Saurav Bansal," Detect and Isolate Jamming Attack in MANET using AODV protocol", International Journal of Engineering Research and General Science , Volume 3, Issue 4, July-August 2015, pp. 590-593.
[17] Chetan Batra, Vishal Arora," RED Strategy for Improving Performance in MANET", Journal of Information Sciences and Computing Technologies (JISCT), Volume 3, Issue 2, April 30,2015, pp. 217-221.
[18] Chaminda Alocious, Hannan Xiao and Bruce Christianson," Analysis of DOS Attacks at MAC layer in Mobile Ad hoc Networks", 11th International Wireless Communications & Mobile Computing conference IEEE 2015, Dubrovnik, Croatia, August 24-28 2015.
[19] R. Akila, Mabel P Jenefer," Efficient Policy based Detection of jamming Attacks in MANETs", International Jouranl of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 5, Issue 3, March 2016, pp. 316-324.
[20] Neeti Yadav and Dr. Vivek Kumar," Securing Ad Hoc Network By Mitigating Jamming Attack", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 4, Issue 6, June 2015, pp. 2502-2506.
[21] Jerome Haerri "Performance Comparison of AODV and OLSR in MANETs Urban Environments under Realistic Mobility Patterns" Department of Mobile Communications, June 2005, pp. 123-134.
[22] Korkmaz G., E. Ekici, F. Ozgüner, and U. Ozgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems in MANET," In Proceeding of the 1st ACM International Workshop on Mobile Ad Hoc Networks, NY, USA, 2004,pp. 76-85.
[23] Lovepreet Singh Shaheed Bhagat Singh Navdeep Kaur," Analysis the Performance of MANET Protocol under Black Hole Attack for E-Mail Application" International Journal of Computer Applications (0975 – 8887) Volume 103 – No.12, October 2014.
[24] Manoharan R., S. L. P. Thambidurai, "Energy efficient robust on-demand multicast routing protocol for mobile ad hoc network," in Proceedings of International Journal of Ad Hoc and Ubiquitous Computing, Vol. 3, 2008, pp. 90-98.
[25] Manvi S., Kakkasageri M.S., Mahapurush , "Performance Analysis of AODV, DSR, Routing Protocols In Mobile Ad hoc Network Environment" In Proceedings of International conference on future Computer and Communication., April. 2009, pp. 21-26.
[26] Meenakshi Patel, Sanjay Sharma,"Detection of Malicious Attack in MANET A Behavioral Approach", IEEE International Advance Computing Conference (IACC)Volume 3,2013,pp.388-393.