ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 9, September 2016

Securing MANET by Eliminating Jamming Attack through Mechanism

Pawani Popli[1], Paru Raj[2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & Prannath Parnami Institute of Management & Technology Hisar, Haryana, India

***Abstract*—**
MANETS endure from power restraints, computational and storage resources, as a result, they are more susceptible to several communications security associated attacks. Thus we try to concentrate on examining and enhancing the security for MANETS. We introduce changes to the AODV we introduce an algorithm to determine the Jamming attack on the MANET routing protocols. These occur by transmitting continuous radio ways to inhibit the transmission between sender and receiver. In our research work we are using an improve CTS/RTS integrated approach to improve the performance of mobile ad hoc networks under jamming attack. The proposed work includes all the routes has unique sequence no. and the malicious node has the maximum Destination Sequence no. and it is the first RREP to reach. So the comparison is built only to the first entry in the table without examining other entries in the table. In proposed mechanism we had taken high mobility network, using with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters, IEEE Along g standard. FTP, Http and VOIP with high data rate are being generated in the network. The solution isolates multiple malicious nodes during route discovery process and assures selection of short and secure route to destination. Simulation results in OPNET to prove the reliability and efficiency of our proposed work. The performance of network is measured with respect to the QoS parameters like throughput, and end to end delay. The results of simulation will demonstrating that the overall performance of MANET under jamming attack will be improved by our proposed approach.

Keywords*:* MANETs, Jamming Attack, Throughput, OPNET.

I. INTRODUCTION

Mobile Ad-Hoc network is an independent system, where nodes/stations are connected with each other through wireless links. There is no limitations on the nodes to join or leave the network, therefore the nodes join or leave spontaneously. Mobile Ad-Hoc network topology is dynamic [1] that can change swiftly because the nodes move freely and can organize themselves arbitrarily. This property of the nodes makes the mobile Ad-Hoc networks random from the point of view of scalability and topology.

Mobile Ad-Hoc network topology is active that can change rapidly and randomly. This possession of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology.

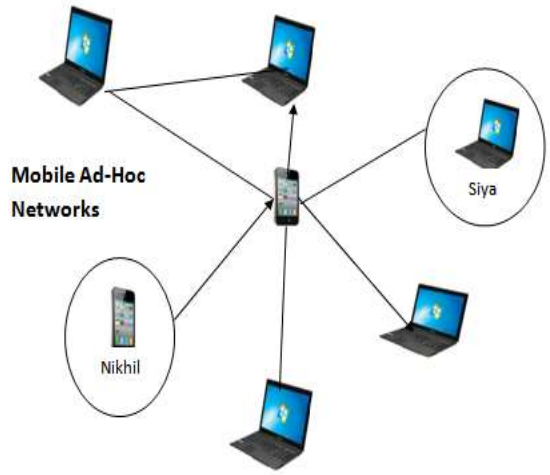

Figure 1: Flow of Data Packets in MANET

Characteristics of MANET

When a node wants to communicate with another node, the destination node must lies within the radio zone of the source node that wants to start the communication. The intermediate nodes within the network supports in routing the packets for the source node to the destination node. These networks are fully self-structured, having the power to work anywhere without any infrastructure. Nodes are autonomous and play the role of router and host at the same time. MANET is self governing, where there is no centralized control and the communication is carried out with blind mutual belief between the nodes on each other. The network can be set up anywhere without any geographical limitations. One of the limitations of the MANET is the fixed energy resources of the nodes.

II. JAMMING ATTACK

IEEE 802.11 one of the most popular attack is jamming attack. Ad-Hoc networks are very prone to security threats. One of the types of Denial of Service (DOS) is Jamming attack. Interferences are caused by jamming

attack. The radio signals are continuously sending in between the transmission which injects the dummy packets and thus causing interferences. Since the radio frequency is an open medium, therefore jamming is big problem for wireless networks. By affecting their throughput, network load, end to end delays etc. Jamming decreases the overall performance of network.

Initially in jamming attack attacker keeps monitoring on wireless media and also verify the frequency at which destination node getting the signals from the sender. Signal is transmitted on that frequency to hinder error free receptor. The main aim of jammer is to trying to get the reception of wireless communications with the physical transmission. A jammer always try to get the legal traffic will completely blocked by constantly emits RF signals to fill a wireless channel.

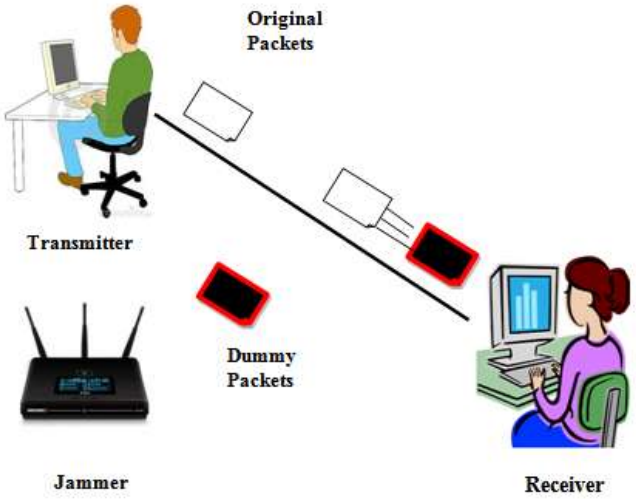

Figure 2: Jammed Scenario in a wireless environment

In this attack jam the transmission channels number of source are formed instead of single source which sends crude packets to the transmission channels and jammed the channel. Because of jamming, packet loss starts. It decreases the efficiency and reliability of the system. Many problems arise due to this attack like channel becomes busy, delay in transmission, new packets being dropped etc. Jamming attacks are mainly divided into two types: Physical and Virtual Jamming. Physical or Radio jamming occur by continuous emission of radio signals or by sending random bits onto the channel and/or at the receiver by causing packet collisions. Virtual jamming can be occurring at the MAC layer through attack on RTS/CTS frames.

III. CTS/RTS MECHANISM

One of the main reason for using the RTS/CTS mechanism [7] is to avoid network level congestion and also prevent and secure the network from hidden jammer node attacks problem from the network point of view. In infrastructure-based networks RTS/CTS mechanism generally works well, in some situations it may lead to unfairness. However, in general setting of ad hoc networks, the RTS/CTS mechanism gives rise to situation where large number of nodes is unable to transmit any packet. These can leads to network-level congestion situations. The Request to Send/Clear to Send (RTS/CTS) mechanism [7] is a handshaking process when hidden nodes are operating on the network that minimizes the occurrence of collisions. Working of RTS/CTS mechanism implementation is illustrated in Figure below

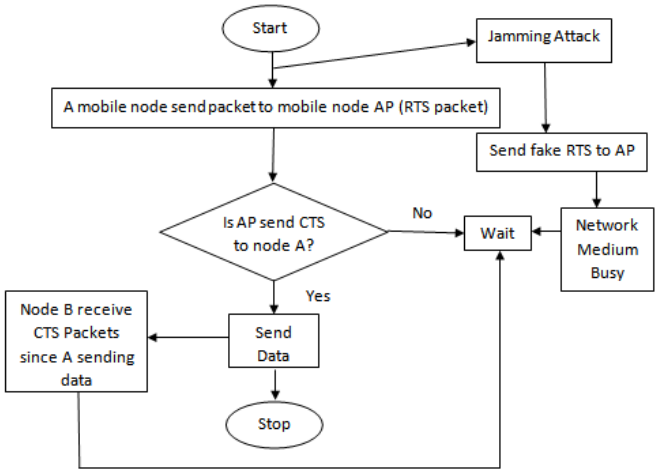

Figure 3: Flow of RTS/CTS mechanism when jamming attack occurs

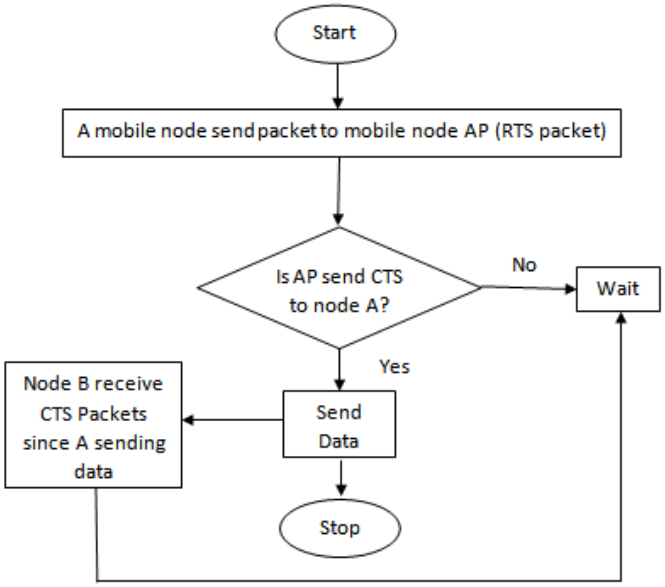

Figure 4: Normal Flow of CTS/RTS

When mobile node A want to send a packet to mobile node AP it initially send a small packet called RTS (Request-To-Send) and replies to it with small packet CTS (Clear-To-Send). After receiving CTS , node *A* sends the *DATA* packet to node *AP*. In-between mobile node B receives the CTS packet since the Mobile Node A is sending data and the mechanism Informs the mobile Node B that the AP is transmitting or receiving data at that time frame and Mobile Node B to wait

for a particular time. Fake RTS frames are sent to the AP mobile node When a jamming attack is launched on the network, that keeps the medium busy or introduces packet collisions causing forced and prevents other nodes from being able to begin with legitimate MAC operations, and repeated back offs.

IV. PROPOSED ALGORITHM

The solution that we introduce here is generally only changes the source node working without changing intermediary and destination nodes by utilizing a method known as Prior_Receive Reply. In this technique three things are appended, a new table RR-Table (Request Reply), a timer WT (Waiting Time) and a variable MN-ID (Malicious Node ID) to the data structures in the actual AODV Protocol.

1. Pre Receive Reply (Packet P)
2. {
3. T0 = Get(Current Time Value)
4. T1= T0 + M_WAIT_TIME
5. While(current time<= T1)
6. {
7. Store P. Dest. Seq No. and P_Node_ID in C_RREP_T Table
8. }
9. While(C-RREP_T is not empty)
10. {
11. Select Dest_Seq_No. from Table
12. If (Dest_seq_No >= Src_Seq_No)
13. {
14. M_node = Node ID
15. Discard entry from table
16. }
17. }
18. Select packet Q for node ID having highest value of Dest._seq_No.
19. Receive Reply (Packet Q)
20. }
21.

ALGORITHM: PRIOR-RECEIVE REPLY METHOD

DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID(M node).

Step 1: (Initialization Process) fetch the current time and add the current time with waiting time.
Step 2: (Storing Process) Store all the Route Response DSN and NID in RR-Table(R) table. Replicate the above procedure until the time exceeds.
Step 3: (Identify and Remove Malicious Node) Fetch the first entry from RR-Table, If DSN is much greater than SSN then drop entry from RR-Table and record its NID in MN-ID.
Step 4: (Node Selection Process) Sort the contents of RR-Table entries according to the DSN choose the NID having maximum DSN among RR-table entries.
Step 5: (Continue default process) Call Receive Reply mechanism of default AODV Protocol. The above algorithm initiates from the initialization procedure, first set the waiting time for the source node to obtain the RREQ coming from other nodes and then append the current time with the waiting time. Then in storing procedure, record all the RREQ Destination Sequence No. (DSN) and its Node Id in RR-Table until the calculated time exceeds. Basically the first route response will be from the malicious node with large destination sequence no., which is recorded as the first entry in the RR-Table. Then compare the first destination sequence no. with the source node sequence no., if there available much more differences among them, certainly that node is the malicious node, immediately eliminate that entry from the RR-Table. This is how malicious node is determined and eliminated. Final procedure is choosing the next node id that has the greater destination sequence no., is achieved by sorting the RR-Table according to the DSEQ-NO column, whose packet is forwarded to Receive Reply method for continuing the default operations of AODV protocol. Additionally, the introduced solution manages the malicious node identity as MN-Id, so that in future, it can drop any control messages coming from that node.

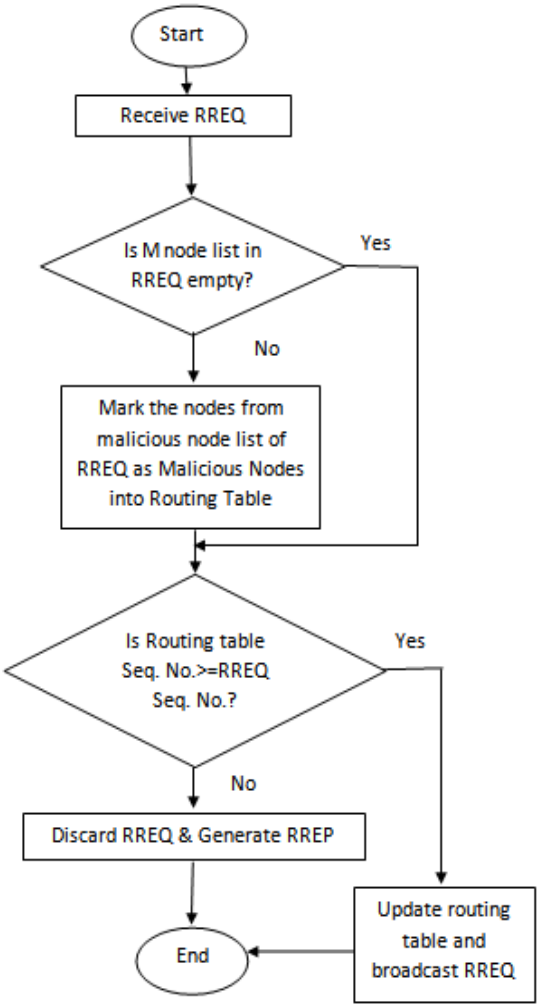

Figure 5: Basic Flow-chart for node broadcasting RREQ

Now however, malicious node is determined, the routing table for that node is not managed.Additionally, the control messages from the malicious node, too, are not sent in the network. Furthermore, for maintaining freshness the RR-Table is flushed once a route request is selected from it[13]. Hence, the operation of the introduced protocol is similar to original AODV, once the malicious node has been determined.

Peak Value = [(Diff.)*(RFR) + No. of Reply Received by Reply Node + Current Simulation Time]/3.

RFR= Total no. of RREP Ratio/Total No. of RREQ Sent.

Where, Diff. = Routing Table Seq. No. – Routing Reply Seq. No.

RFR= Reply Forward Ratio

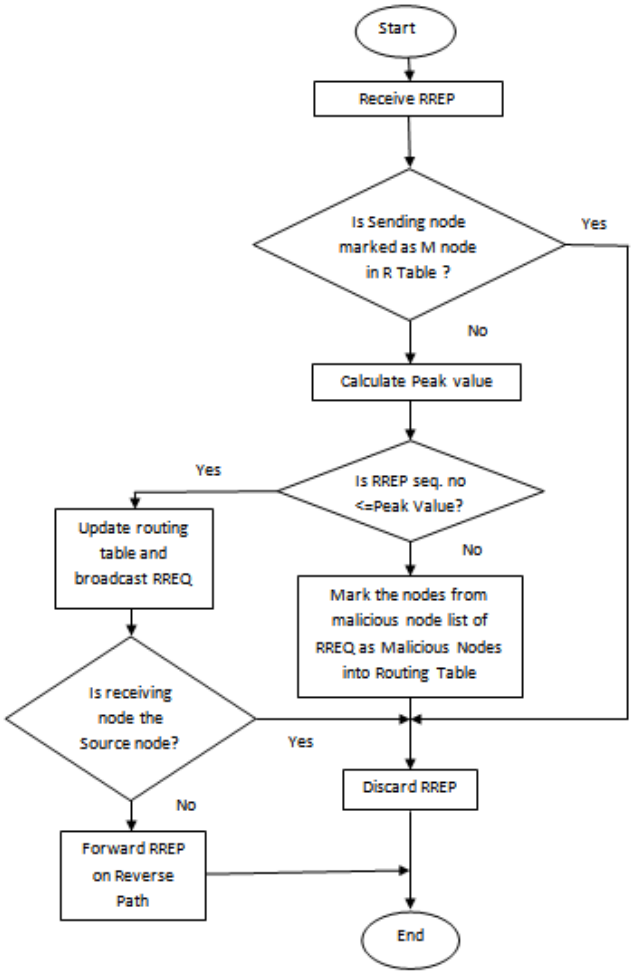

Figure 6: Flow-chart for node receiving RREP

Table I: MANET Simulation Parameters for Jammers

Examined Protocols Cases	AODV with Jamming Attack
Number of Nodes	150 and 200
Types of Nodes	Mobile
Simulation Area	1500*1500 m
Simulation Time	3600 seconds
Mobility	Uniform(10-100) m/s
Pause Time	200 seconds
Performance Parameters	Throughput, Delay
No. of Jammers	10
Jammer Bandwidth	100,00
Jammer band base Frequency	2,302
Jammer Transmitter Power	0.001
Trajectory	VECTOR
Long Retry Limit	3
Max Receive Lifetime	0.5 seconds
Buffer Size(bits)	25600
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Traffic type	FTP, Http
Active Route Timeout	3sec.
Hello interval(sec)	1,2
Hello Loss	3
Timeout Buffer	2
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	53 Mbps
Transmit Power	0.005
RTS Threshold	1024
Packet-Reception Threshold	-95

V. RESULTS

After presenting the basic results of all simulations carried out in both scenarios, in this paper, we analyse and discuss all these results. The performance metrics collected and presented in our results are either based on

the object statistics or global statistics of the MANET model i.e. the entire network. In representing these data, we presented the average or time average values of the results in this report. We start our discussion and analysis with the two main scenarios in which the first scenario contains 150 mobile nodes and the latter holds 200 mobile nodes. In each scenario, we did two simulations of a regular network operation in MANET and Jamming attack to be precise in MANET. All simulations i.e. both scenarios were run for a time period of 20 minutes, which ranged from 0 to 1200 seconds as shown in the result graphs. After that, we analyse and compare within each scenario and also both scenarios based on their throughput and end-to-end delay. Basic parameters used for experimentation with OPNET simulator. Area for communication is 1500 x 1500 m with 150 and 200 mobile nodes. The performance comparison of three scenarios in term of throughput is explained in figure The overall simulation performance is presented in nutshell in the following table, which indicates that the elimination of jamming attack scenario provides the better results and try to normalize the jamming effected network to its normal state as close as possible

.

5.1 Throughput:

Throughput can be defined as the ratio of the total amount of data reaches from source to a destination. In other words time taken to receive the last message by the destination is called as throughput. It can show as bytes or bits per seconds (byte/sec or bit/sec). There are some components that affect the throughput such as; changes in topology, availability of limited bandwidth, unreliable communication between nodes and limited energy. A high throughput is absolute choice in every network. Figure represents the graph that show the throughput in bits per seconds. The x-axis denotes the simulation time in minutes and the y-axis denotes throughput in bits per seconds. Scenario 1, represents the scenario with no malicious event and normal network state, scenario 2 represents the jamming attack network and scenario 3 represents the mobile jammers and implementation of the proposed method. It can be clearly seen, that the overall throughput is decreases when jamming attack arise in comparison to the normal network state. However, the entire network throughput is increased once the proposed unified mechanism is implemented.

Table II: Throughput of all three scenarios at 150 and 200 nodes

No. of Nodes	Without Jamming	With Jamming	Jam Removal
150	3566213	3227315	3428088
200	14563478	10435675	14206537

In first scenario of 150 nodes of our experimentation, packets travels are shown as throughput with peak value of approx. 3566213 bits per seconds and it is represented as bits per second.

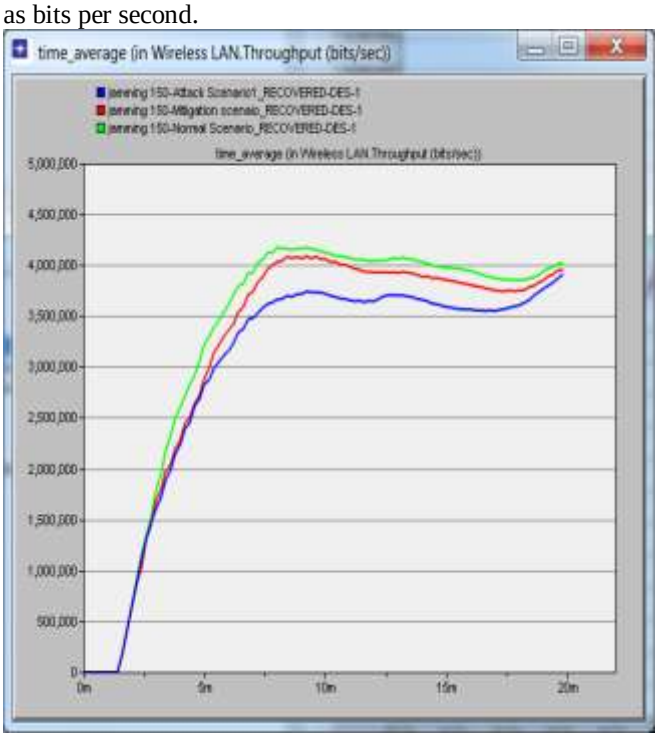

Figure: 7 Throughput of all three scenarios at 150 nodes

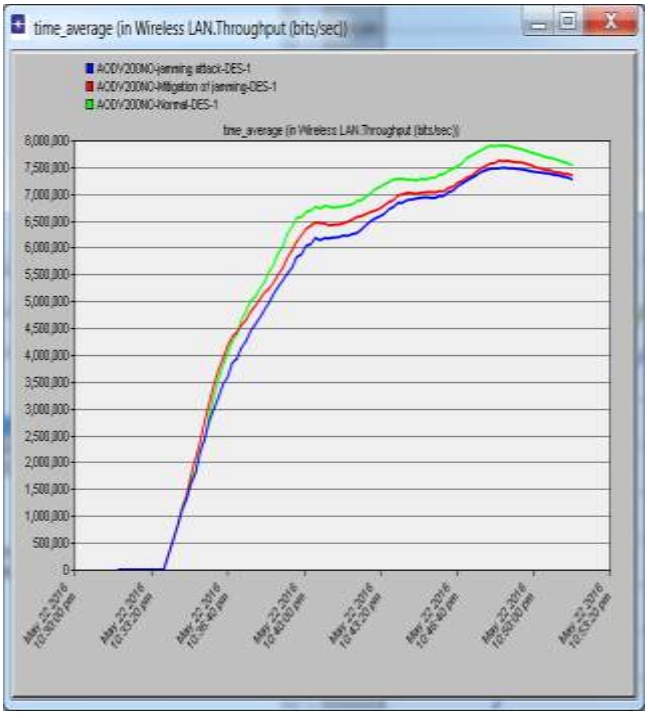

Figure 8: Throughput Of All Three Scenarios At 200 Nodes

In second scenario which is with jamming attack, packets drops which are acted as throughput, decreases to value of approx. 3227315 bits per second. In first scenario of 200 nodes of our experimentation, packets travels are shown as

throughput with peak value of approx. 14563478 bits per seconds and it is represented as bits per second. In second scenario which is with Jamming attack, packets drops which are acted as throughput, decreases to value of approx. 10435675bits per second.

This drop of packets in form of throughput is due to the jamming effect. The recovery of the throughput takes place with proposed mechanism by elimination of the jamming attack as throughput is increased in comparison to jamming attack but not up to the normal scenario.

5.2 End To End Delay:

The packet end to end delay is the average time that packets take to traverse in the network. This is the time from the generation of the packet by the sender node up to their reception at the destination and is expressed in seconds. Hence all the delays in the network are called packet end-to-end delay. It includes all the delays in the network such as propagation delay (PD), processing delay (PD), transmission delay (TD), queuing delay (QD).

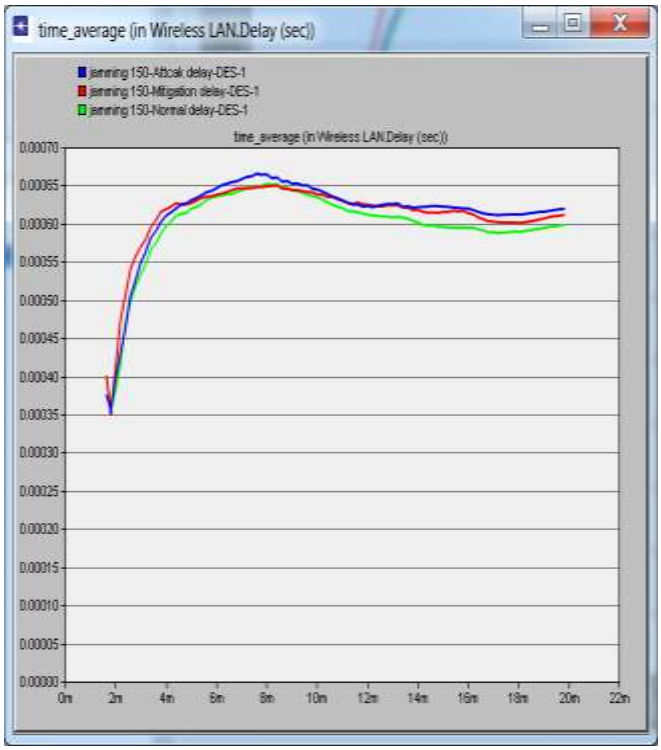

Figure 9: Delay of All Three Scenarios at 150 Nodes

In first scenario of 150 nodes of our experimentation, packets Delay are shown as figure 5.3 with peak value of approx. 0.0010 seconds. In second scenario which is with jamming attack, packets delay Increases to value of approx 0.35 seconds.

In first scenario of 200 nodes of our experimentation, packets delay is approx. 0.0020 seconds. In second scenario which is with jamming attack, packets delay increases to value of approx. 0.30 seconds.

The recovery of the end to end delay decreases with our proposed mechanism by elimination of the jamming attack as end to end delay comes to similar to the value 0.000256 seconds. Thus our proposed mechanism eliminates jamming attack in network.

Table III: Delay of all three scenarios at 150 and 200 nodes

No. of Nodes	Without Jamming	With Jamming	Jam Removal
100	0.000598	0.000614	0.000610
200	0.0009	0.0011	0.0010

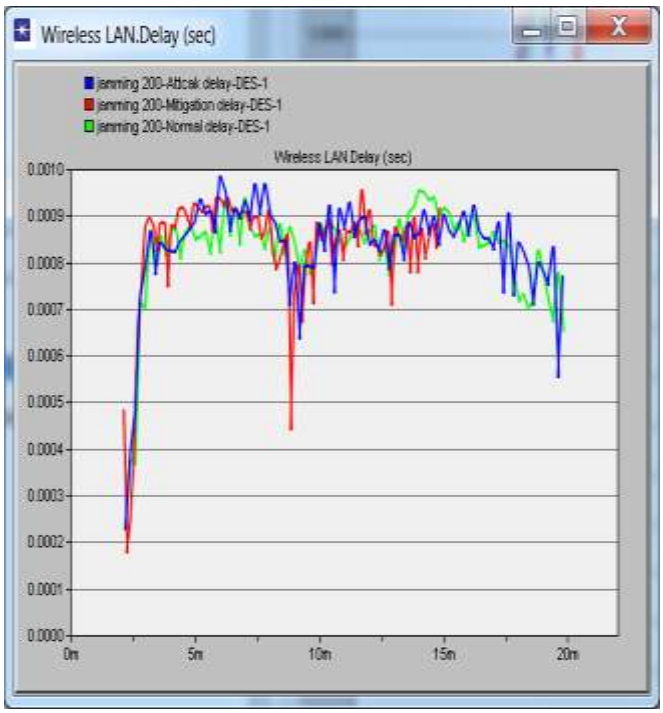

Figure 10: Delay of All Three Scenarios at 200 Nodes

CONCLUSION

Jammers attacks will have an effect on network's performance as a result of the jammers interferes with the traditional procedure of the network. The effect of attackers studied in this paper was by increasing delay, data dropped traffic found and sent and decreasing packet drop ratio of the network. In this research work, the network performance under jamming attack is studying by applying improved RTS/CTS approach. The unified mechanism is imposed on the selected nodes on the network and deployed on the particular area. The findings of the research clearly states that, the implementation of such unified mechanisms have a significant impact on the overall network through positively. The unified mechanism that contains improved RTS/CTS that shows adequate performance in MANET. Since several mobile jammers used in this simulation experiment, the proposed security mechanism satisfactorily mitigated the effects of the

jamming attack on the network and increased the overall performance of the network while improving data drop rate. The data dropped rate decrease successfully. Since the jamming attack leads packet drop rate and low throughput impact on the network, the rate of delay seems acceptable on the network.

FUTURE WORK

We consider future research works focused on using real time attacks which is needed to ascertain greater degree of detection of particular vulnerabilities in both Mobile and ad hoc networks. Based on the attack classifications in various levels described in this work, we can use improved version of IDS and also by integrating IDS mechanism and Behaviour Filter to analysis the result. However based on our simulations and for more accurate results we implement this into OPNET Modeler.

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.

[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.s

[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.