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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Enhanced Scheme for Mitigating Jamming Attacks in MANETs

Madhvi[1], Nisha Pandey[2]

M.Tech CSE Student, Department of Computer Engineering, Shri Ram College of Engineering and Management, Palwal, Haryana, India[1]

Assistant Professor, Department of Computer Engineering, Shri Ram College of Engineering and Management, Palwal, Haryana, India[2]

ABSTRACT: Mobile ad hoc network (MANET) is a set of wireless nodes that dynamically self-organising into a changeable topology to design the network using any preceding framework. Due to open nature of wireless communication medium, wireless networks are susceptible to jamming attacks. Jammers interfere with the legitimate nodes by sending strong jamming signals. Legitimate nodes can successfully transmit only between the gaps of the jamming signals. Thus, it is important to detect and mitigate a jamming attack as soon as it happens in order, to effectively take counter measurements. There are various types of jamming, but the signature of jamming attack is to degrade the performance of the network. Based on this observation, we proposed an enhanced scheme for mitigating jamming attack using bandwidth and packet delivery ratio algorithm. Using OPNET simulation, the attack can be detected through increase in performance criteria and successfully mitigated by our proposed scheme. We have analysed the results using OPNET 14.5 simulator.

KEYWORDS: Jamming Attack, DoS Attack, MANET, AODV, OPNET.

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) can be defined as collections of autonomous mobile nodes, which communicate wirelessly without any need for pre-existing network infrastructure. In addition, MANET do not rely on centralized control [6,10]. Each node participating in the MANET is not only regarded as an end system but also as a router relaying messages to other participating nodes. MANET are self-configuring and the nodes form a dynamic topology as represented in figure 1. As the nodes move, they can organize themselves on the fly and hence the topology of MANET may be subject to frequent and unpredictable changes. MANET can be utilized in campus and conference environments, on railways, remote areas without communication infrastructure or areas where the communication infrastructure is down due to natural disaster or political tensions [6]. The number of users in each scenario can range from about 10 nodes in emergency settings, to hundreds of people in a campus or conference setting, to thousands of participants in political unrest or military settings.

Because the transmission medium is open to any transmitter, wireless networks are easily subjected to jamming attacks. Therefore, jamming is a major threat to wireless security.Jamming is a notable feature of denial-of-service (DoS) attacks. Jamming drives, electromagnetic energy towards a communication system to prevent signal transmission. In wireless networks, jamming interferes into the radio frequencies used by network nodes [7,9].

Jamming is the main reason for many problems in the real-world applications. For example, in border security, an intruder has an abilityto prevent the communication and cross the border without being detected [8].Thus,an unwanted environment, it is very important to detect the place where the channel is jammed or deliver the messages out of the jammed area.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

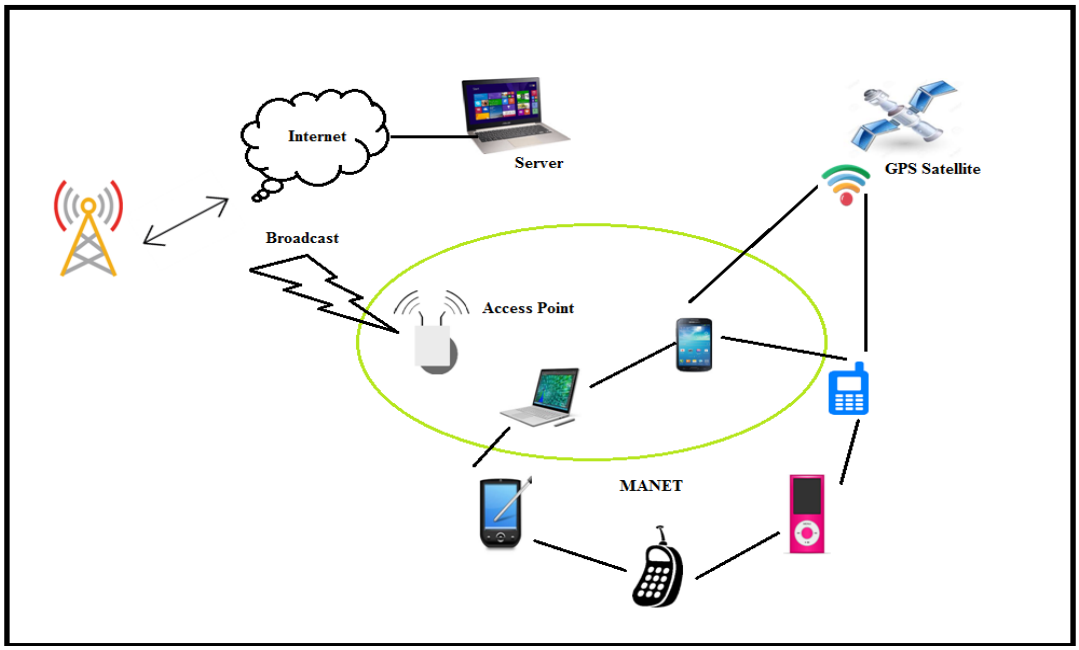

Fig.1: Mobile Ad-Hoc Networks

II. RELATED WORK

Hongjiu Yang et.al [1]- In this paper, authors studied a countermeasure for wireless networked control system suffering from jamming attacks in cyber layer by a variable sampling approach. They utilized the stackelberg game approach to analyse interactions between users and jammers. They also designed a variable sampling controller that deal with data packets dropout. At last, authors validated the effectiveness of the proposed methodology by using a simulation numerical which was stable in the mean square sense.

Mohammad Amin Maleki Sadr et.al [2]- In this, authors surpassed the jamming effect and estimated jamming channel state information by using Kalman filtering approach. They designed the beam forming weights in relay nodes in which achievable rate was maximized to the condition that the total relay power transmission would be below a specific threshold level, which provides a closed form solution for a QCQP type problem. For simulation they used 20 relaynodes. Authors concluded that attacker channel estimation achieves Cramer Rao identical performance as compared to full CSI method with very low computational complexity.

S.G. Hymlin Rose et.al [3]- Here, authors proposed a new technique to detect jamming by utilizing clustering approach and time-stamping. In this approach, jamming node was identified by time-stamping method when its value exceeded by threshold and also by calculating packet delivery value. Authors designed a system architecture in which spreading code was used for receiving acknowledgement, if matched with receiver, also identified as malicious node. For simulation they used MATLAB and number of nodes 20 and transmission range within 250m. Performance metric was analysed based on packet delivery ratio. After the results, authors concluded that proposed approach was simple and if any node was identified as a malicious node then communication was altered to other grouping by arranging a new cluster and hence transmission was not disputed as well as within the increase of malicious node the packet delivery ratio decreases and vice- versa.

Xianglin Wei et.al [4]- Here, authors presented a jamming detection algorithm based on association graph. According to them, the proposed algorithm was consisted of two phases i.e. learning and detection phase in which initial new symptoms were extracted and calculated through eliminating overlap and association graph was derived for the detection of jamming attacks. For simulation they used NS-3 simulator having several parameters like simulation area of 400m*400m, two routing protocols OLSR and DSDV. Authors took three network performance metrics: PDR, PSR and SNR. After the simulation, authors derived that almost all nodes in network detect the existence of jamming nodes

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

and distinguish different jamming models but detection performance in OLSR was better than DSDV algorithms due to differences in routing algorithms.

Ali Aldarrji et.al [5]- Here, authors proposed an upgraded countermeasure method for jamming attacks by using polarized beam forming with a planar array. The proposed strategy was composed utilizing the Linearly Constrained Minimum Variance (LCMV) paradigm. For execution assessment, signal to impedance proportion was set to be - 20dB and assessed in terms of Bit Error Ratio (BER) to evaluate its data uprightness and antijamming qualities through different antenna array sizes. Authors incorporated both polarization and space data to stifle undesired obstruction. After the outcomes, authors inferred that proposed beam former basically upgrades the information system execution when the jammer and wanted signal are found eagerly in space area. Likewise, the greater the array estimate, the less information botch happened.

III. PROPOSED ALGORITHM

The proposed algorithm consists of the following main steps-

Step 1 (Route Discovery) - Sender node sends route discovery packet for the receiver node to identify the routes/path available for the establishment of communication in the network.

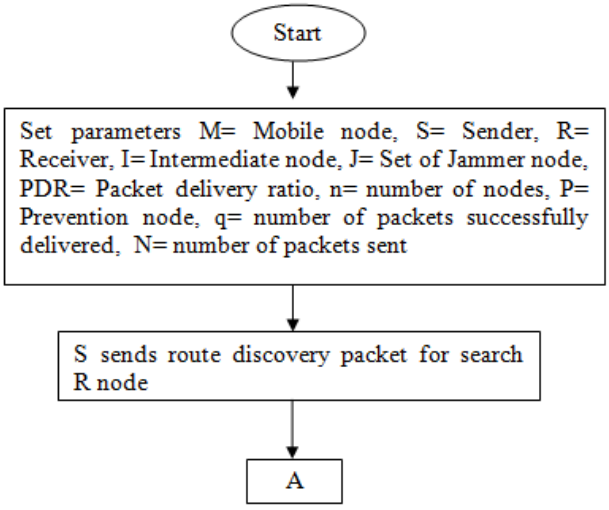

Fig.2: Flowchart- Route discovery

Step 2 (Fetching data) - After identification of routes, if receiver node incorporate morethan one path or route then data has to be send and in between transmission of data if the intermediate node behave as a jammer then the intermediate node generate false dummy packet and broadcast them in to the network and drops the data which was received from source or others intermediate node.

Step 3 (Find jamming node) - Find the jammer node by the help of incoming data and outgoing data. If the value of incoming data is greater than outgoingdata, then node will set as jammer and prevention node whose role is to prevent jamming by sending warning messages to jammer node i.e. not to spread jamming in the network. Further, if jammer node continually spread jamming, then it will be block and prevention node sends message to source node to forward the data through other inter mediatory nodes.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

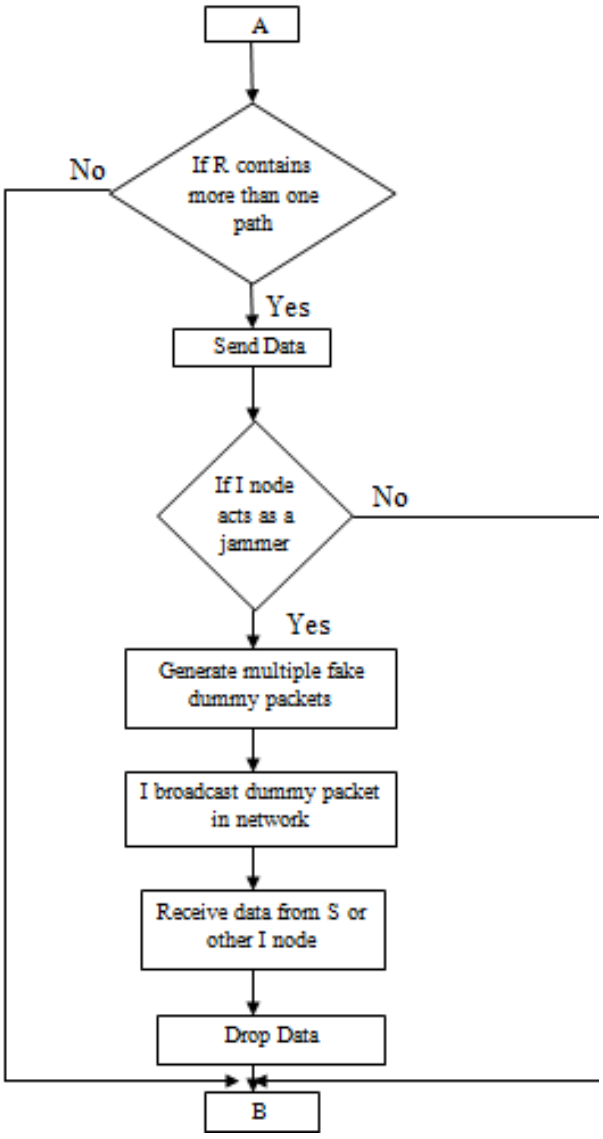

Fig.3:Flowchart- Fetching data

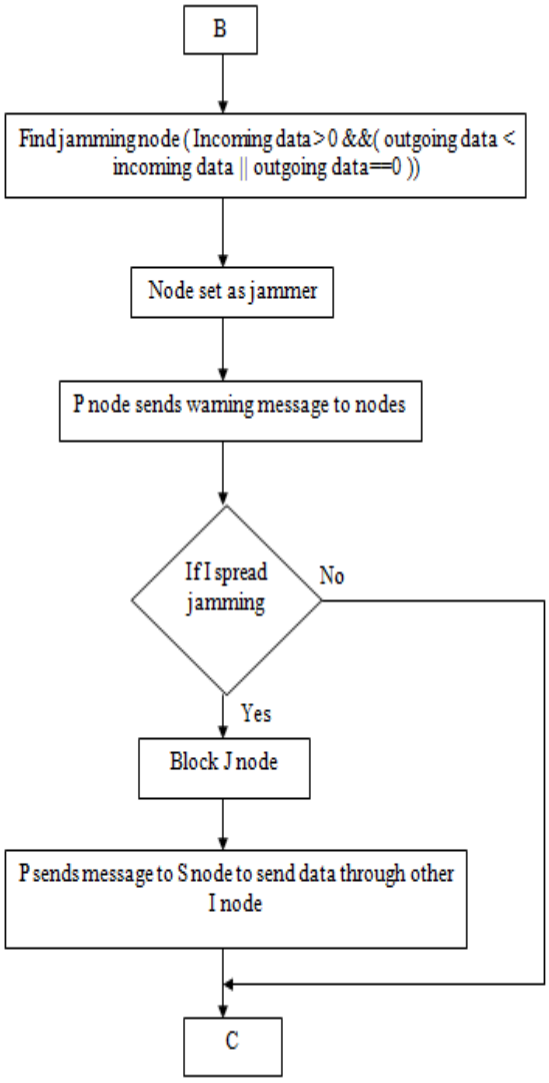

Fig.4:Flowchart- Find jamming node

Step 4 (Calculate PDR) - Here reliability of intermediate nodes is measured by calculating the packet delivery ratio with the help of prevention node and queue is used for storing the data.

Step 5 &6 (Continue default process) - Process of route discovery and finding jamming node will be repeated for n number of nodes.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

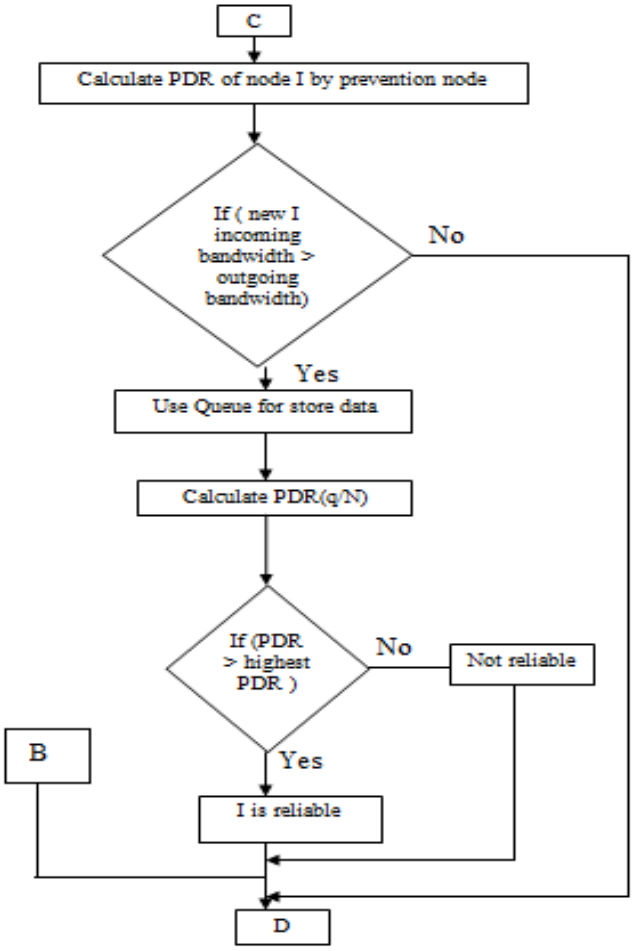

Fig.5: Flowchart- Calculate PDR

Step 7 (Final result) - At last, when all jamming nodes in the will found then prevention node block them and they will not be able to participate in further communication.

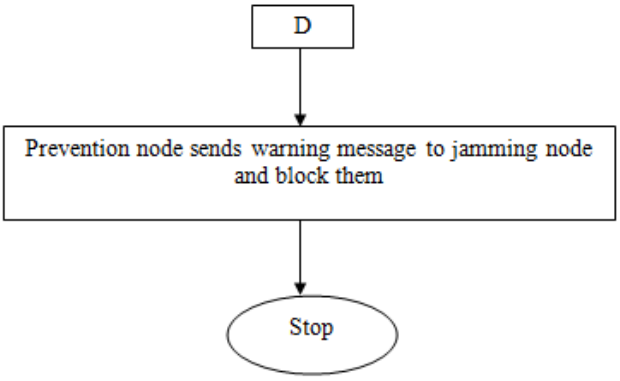

Fig.6:Flowchart- Final Result

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

IV. IMPLEMENTATION AND SIMULATION RESULTS

A. IMPLEMENTATION-

Implementation of Jamming Detection and Mitigation Strategies done in OPNET 14.5 simulator. Various simulation parameters were used like data type- constant bit rate, packet size- 512 bytes, number of jammers-10, jammer bandwidth-100000, trajectory- vector, pause time-10 seconds. Some important parameters were listed in below table 1-

Table 1. Simulation parameters used in implementation

Parameter	Value
Number of nodes	150, 175, 200
Simulation time	1500 seconds
Simulation area	50km*80km
Mobility model used	Random waypoint
Mobility	Uniform(0-20) m/s

B. RESULTS-

The simulation result shows the performance behaviour of jamming attack mitigation in terms of throughput having varying nodes. It can be clearly seen, that the jamming attack decreases the overall network throughput in comparison to the normal network state. However, the entire network throughput is increased once the proposed unified mechanism is implemented. In addition to this, the state of the throughput in mitigating jamming is more than the normal jamming scenario.

Figure 8,9 and 10 illustrates the scenarios using different number of nodes and performance of the network based on the throughput. Here, the x-axis represents the simulation time in minutes while the y- xis represents the throughput in bits per seconds.

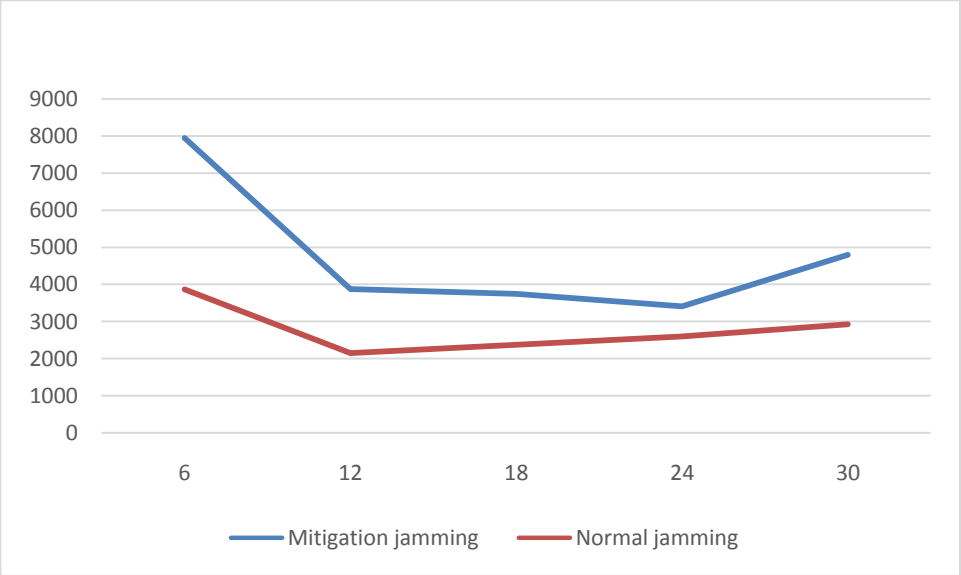

Fig.7: Comparison of Throughput having 150 nodes for normal and mitigation jamming

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

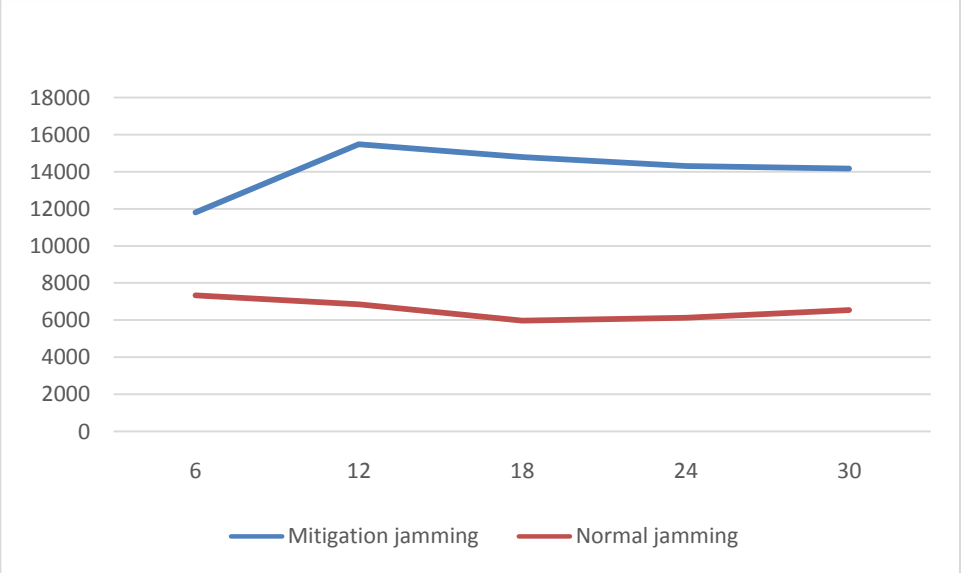

Fig.8: Comparison of Throughput having 175 nodes for normal and mitigation jamming

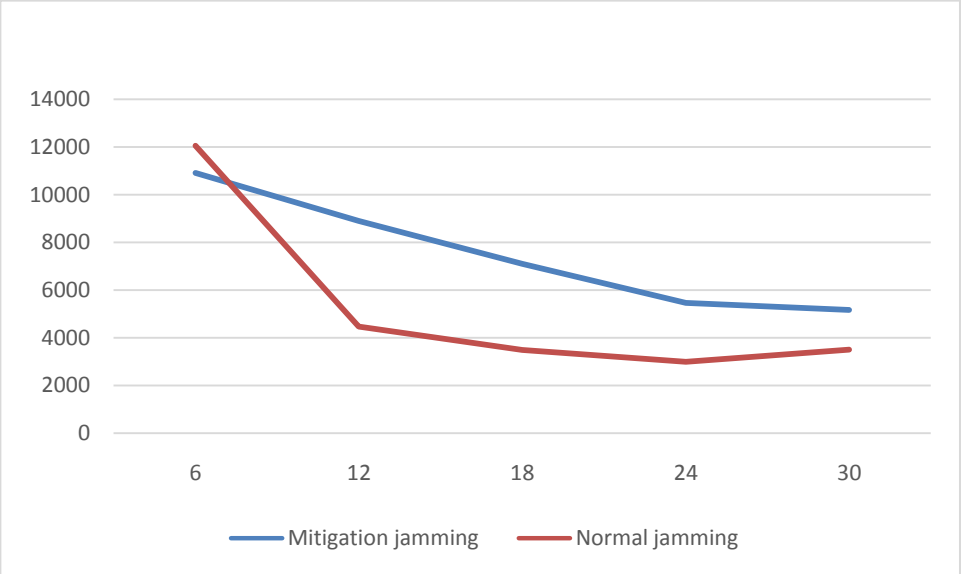

Fig.9: Comparison of Throughput having 200 nodes for normal and mitigation jamming

V. CONCLUSION AND FUTURE WORK

In this, we proposed a new enhanced scheme to mitigate jamming attack in MANET. The findings of the research clearly state that, the implementation of such a scheme have a significant impact on the overall network positively. On the other hand, the implementation of such scheme does not only mitigate the jamming attack effects, it also increases the overall performance above the normal state of the network. In case of 150 nodes the throughput was improved about 40-45% as compared to normal jamming scenario while 50-55% having 175 nodes and28-32% having 200 nodes. As a part of future work, we may want to perform out the simulations with diverse transmission scopes of

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

mobile nodes and with various number of jammer nodes utilized by attacker at the same time also some other routing protocol can be deployand corresponding results can be compared.

REFERENCES

1. Yang, H., Shi, M., Xia, Y., and Zhang, P., "Security Research on Wireless Networked Control Systems Subject to Jamming Attacks" , IEEE Transactions on Cybernetics, pp.1-10, 2018.
2. Sadr, M.A.M., Attari, M.A. and Amiri, R., Robust Relay Beamforming Against Jamming Attack ", IEEE Communications Letters, Vol.22, Issue 2, pp.312-315, 2018.
3. Rose, S.G.H., and Jayasree, T., "A Jamming Detection Technique For WSN Using Timestamp", IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), 2018.
4. Wei, X., Sun, Q., Hu, F., and Wang, T., "Association Graph based Jamming Detection in Multi-Hop Wireless Networks" , IEEE International Conference on Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC) ,pp.397-402, 2017.
5. Aldarraji, A., Hong, L., and Shetty, S., "Polarized Beamforming for Enhanced Countermeasure of Wireless Jamming Attacks", IEEE 35th International Performance Computing and Communications Conference (IPCCC), 2017.
6. Rahman, F.H.M.A., and Au, T.W., "Impact of IPsec on MANET", IEEE International Symposium on Computer, Consumer and Control (IS3C), pp. 408-411, 2016.
7. Houssaini, M.A.E., Aaroud, A., Horea, A.E., and Othman, J.B., "Detection of Jamming Attacks in Mobile Ad Hoc Networks using Statistical Process Control", ScienceDirect The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016), Vol.83, pp.26-33, 2016.
8. Ahmed, D.E.M., and Khalifa, O.O, "An Overview of MANETs: Applications, Characteristics, Challenges and Recent Issues", ResearchGateInternational Journal of Engineering and Advanced Technology (IJEAT), Vol.6, Issue 4, 2017.
9. Bhojani, R., and Joshi, R., "An Integrated Approach for Jammer Detection using Software Defined Radio", Science Direct International Conference on Communication, Computing and Virtualization, Vol. 79, pp.809-816, 2016.
10. Chowdhury, S.K., and Sen, M., "Attacks and mitigation techniques on mobile ad hoc network- A survey", International Conference on Trends in Electronics and Informatics **(**ICEI), 2018.