# Detection and Prevention Scheme against Jamming Attack in MANET: A Survey

Nidhi Ghodki[1], Deepanjali Joshi[2], Ravi Singh Pippal[3]
[1]M-Tech Research scholar, [2]Research Guide, [3]HOD of CSE Department
Radharaman Engineering College Bhopal, India

***Abstract- Mobile Ad hoc Network (MANET) has the ability to communicate each other without any fixed network. It has the unpleasant habit to take decisions on its own that is autonomous state. MANET is infrastructure less. An integrated security solution is very much needed for networks to protect both route and data forwarding operations in the network layer. Security is an extremely important requirement in MANET. Without any suitable security in network, then malicious node inside the network will act as a normal node which causes heavy flooding of control packets and this flooding is start to a few number of packets and after some time the massive number of packets are flooded in network i.e. generally known as jamming attack. In this research we will proposed the security scheme against jamming occurred in the in MANET. Jamming attack is one of the attacks in physical layer in terms of signals or bits, MAC layer in terms of channel access, bandwidth allocation and in network layer in terms of heavy control packets. This attack is comes under security acting attacks in MANET.***

***Index Term- Jamming, Routing, Security, MANET.***

## I. INTRODUCTION

A mobile ad hoc network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service detection without the help of an establishment infrastructure. Nodes of an ad hoc network be confident on one another in forwarding a packet to its stop (terminus), due to the limited range of each mobile host's wireless transmissions. Security in MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Unrelated (distinct) networks using dedicated nodes to support basic functions like packet forwarding, routing, and network guidance, in ad hoc networks those functions are carried out by all available nodes[1]. This very difference MANET can be established extremely flexibly without any fixed base station in combat zone, military applications, and other emergency and disaster situation. Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange.

The whole procedure of attack behavior and identification are represents by figure 1. Here the black red node represents the heavy flooding of packets with dotted bolt.

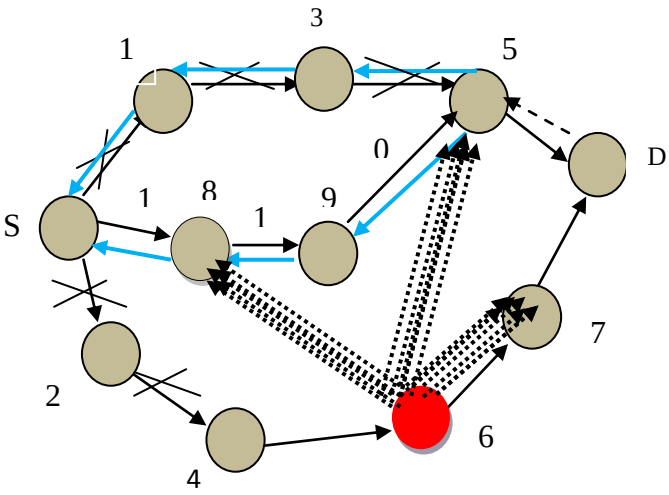


Fig.1 show whole procedure of attack

Every packet in MANETs has a unique identification number. This number is an increment value, i.e., the next packet must have higher value that the current packet identification number. The node in regular routing protocols keeps the last packet identification number that it has received and uses it to check if the received packet was received before from the same originating source or not. The jamming attackers are completely jammed the capability of data forwarding. IDS identify heavy data flooding of only a single or multiple attackers that are floods heavy traffic. It means it is the only sender that do that kind of activity in network. This solution provides a fast and reliable way to identify the apprehensive reply. No overhead will be added to the channel because the identification number itself is included in every packet in the base protocol.

## II. JAMMING ATTACKS

Jamming is one sort of denial of service attacks in the wireless communication, which disrupts the operation of physical or link layers in legitimate nodes by transferring illegitimate signals. Jamming is one of such "availability attacks which can be easily carried out. It is defined as the intended transmission of radio signals that disrupt legitimate communication by decreasing signal to noise ratio. The author in [2], define the traditional jamming & propose taxonomies of jamming attacks & countermeasures in wireless networks. The author in [3], define the selective jamming attack is active in short time period and that prevent scheme is real time packet classification at the physical layer. The author in [4], introduced switched beam directional antennas in wireless sensor network.

### *A. Jamming Attack Models*

Jammer can perform various different attack strategies in order to interfere with other wireless communication.

As a phenomenon of their different attack philosophies, these various attack models will have different levels of effectiveness, and may also require different detection strategies. Some possible strategies are expressed below [5]:

*Constant Jammer:* Constant jammer continuously sends out random bits to the channel without following any MAC-layer etiquette. Specifically, the constant jammer does not wait for the channel to become idle before transmitting. If the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer, a constant jammer can effectively avoid legitimate traffic sources from getting hold of channel and sending packets.

*Deceptive Jammer:* it is different from continues jammers. Instead of sending out random bits, the unreliable jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions.

*Random Jammer:* Instead of continuously sending out a radio signal, a random jammer is alter change between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time, and in the second mode (sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.

*Reactive Jammer:* In the reactive jammer, it is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet (dumb)when the channel is idle (enactive), but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. We would like to point out that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. The primary advantage for a reactive jammer, however, is that it may be harder to identify.

### *B. Security Goals:*

Security means a set of transaction that are satisfactory funded. In MANET, all networking functions are performed routing and packet forwarding, by nodes themselves in a self-organizing manner. Self-organizing is a problem for security in mobile ad -hoc network. The goals to evaporate if mobile ad-hoc network is secure or not are as follows:

*Availability:* Availability means the assets are accessible to authorized parties at applicable times. Accessibility applies both to data and to services. It ensures the superficiality of network service despite denial of service attack.

*Confidentiality:* Confidentiality ensures that computer-related assets are accessed only by approve parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some trusty information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called retirement or privacy.

*Integrity:* Integrity means that assets can be modified only by authorized parties or only in permitted way. Qualification includes writing, change status, deleting and creating. Goodness assures that a message being transferred is never corrupted.

*Authentication:* Authentication enables a node to ensure the identity of peer node it is communicating with. Confirm is essentially declared that participants in communication are authenticated and not impression. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

*Non repudiation:* Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

*Anonymity:* Anonymity means all facts (inside story) that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

## III. LITERATURE REVIEW

[6] ON a New Type of Denial of Service Attack in Wireless Network: The Distributed Jammer Network.

Hong Huang et al. present a new type of denial of service attack (DJN) to wireless network. DJN in combination of large no. of tiny low power jammers motivated by the advancement in radio technology. DJN can cause a phase transition in target network performance even when the total jamming power is constant and investigated the impact of DJN topology on the jamming effectiveness.

[7] Detection of Jamming Attacks in Wireless Ad hoc Networks Using Error Distribution.

Ali Hamieh and Jalel Ben-Othman Present one main challenge in design of this network: Define the jamming attack in MANET & also provide the detection method by the measurement of error distribution. The introduced is their vulnerability to denial of service attacks. This paper is considering a class Dos attack is called a jamming, and in this paper use IEEE 802.11 MAC layer ad hoc n\w is used for security. In this paper are used constant jammer are continuously emits radio signal that represents random bits, and use the distributed coordination function to MAC. DCF performance explain a Distributed access algorithm based on CSMA/CA. The aim of minimize the collision. Correlation coefficient is detection of jamming attack measure in jamming attack case is greater than in normal n\w activity.CC is given the static measure of relation between two random variable. Proposed model advantage are simplicity and efficiency for detecting jamming attack. Also as this model is passive and there is no communication overhead, the required storage and computation overhead is very small.

[8] Mitigating Inside Jammers in Manet Using Localized Detection Scheme.

Ajana J.[1], Helen K.J. [2]. They proposed a distributed jamming detection scheme known localized detection scheme (LDS) for jamming attack. In this all node inside it, detect jammer as using the basic parameters like delivery ratio and signal strength .LDS scheme give better performance as compare to traditional approach and this approach consume a constant energy as compared to others.

[9] AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Network.

Yu Zhang et al. developed a comprehensive system called audit–based misbehavior detection .AMD(Audit Misbehavior detection) provides a comprehensive misbehavior, identification and node isolation system for eliminating misbehavior from n\w. AMD isolates effectively and efficiently both continues and selective packet droppers. AMD isolates is implementing a reputation module is responsible for computing and managing the reputation node and trustworthy routes discovery and identification of misbehaving nodes based on behavioral audits. AMD detect selective dropping attacks even if end to end traffic encrypted and can be applied to multitechnique n/w model process of identifying misbehaving nodes as Renyai-ulam game, and derived resource efficient identification Strategies. AMD can detect selective dropping attacks over end to end encrypted traffic streams and detect network operation.

[10] Detection and Prevention of various types of Jamming Attacks in Wireless Networks.

Mr.Pushphas Chaturvedi and Mr. Kunal Gupta present detection and prevention of various type jamming attack in the wireless network and this attack is the broadcast in nature. Jamming is disrupt the wireless transmission and the jamming is unintentionally by n/w and intentionally in from attack. It is interference noise or collision the receiver end. Detection scheme use the monitoring mechanism. It is observe the detecting potential malicious activity by jammer. And the subset of node M that will act as network monitor and employment of a detection algorithm apply each monitor node. Prevention is used rate adaptation scheme and mapping to commitment scheme for selective jamming attack prevention packet hiding methods can also be used for jamming prevention.

[11] Measures and Countermeasures for Null Frequency Jamming of On-Demand Routing Protocols in Wireless Ad Hoc Networks.

M. Balakrishnan et al. In this paper low radio jamming method NFJ introduced to target the protocol operating periods and disrupt network communication. Null frequency jamming is the periodic attack targeting protocol or frequency of operation is referred to as NFJ. This paper aim to test the hypothesis by investigating through NFJ targeted at the use of on-demand routing protocol for ad hoc n/w. It analysis the mathematical simulation result show substantial degradation in end to end n/w throughput at certain NF. Jamming is the self synchronizes with the route recovery cycle. We study an effective countermeasure randomized route recovery periods and mitigating the impact of NFJ. The basically NFJ is to create a burst of packet losses subsequence pushing the n/w protocols into the recovery node, describes NFJ low radio at the routing layer using simulations and analytical modeling.

[12] ON the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks.

Konstantionos Pelechrinis et al. This paper present efficacy of frequency hopping coping with jamming attack. FH as an anti-jamming this paper examine effectiveness of FH. In this game theoretic framework capture the interaction between a links and jammer employ FH. And present framework how can apply on 802.11 network to quantify the efficacy of FH, Also show that if the no. of orthogonal channel large then frequency hopping will be very effective in coping.

[13] Surviving Attacks in Challenged Networks.

Jordi Cucurull et al. This paper present surviving attack in challenged network. That means a disaster event inside the telecommunication infrastructures can be easily damaged or overloaded, this time movement action network provide the communication services in ad hoc manner. This paper are proposed a general security framework for monitoring and reacting to disruptive attacks. Paper are presented modular framework for attack survivability in intermittent connected MANET composed of detection, diagnosis, mitigation and adaptation components.

[14]Improving Reliability of Jamming Attack Detection in Ad hoc Networks.

Geethapriya Thamilarasu et al. In this paper present improving reliability of jamming attack detection. The denial of service attack is attacked in any security system and affected the availability of a node or entire network. In this paper focuses on jamming attack at physical and MAC layer in based on the 802.11 Ad-Hoc network. Collision occur in wireless network by jamming attack, and the hidden terminals interferences and n\w congestion. In this paper present a probabilistic action analysis to show, that collision occurrence definitively determine jamming attack in channel. Then first investigate the problem discover and what is wrong the presence of jamming in ad-hoc n\w. Then evaluate the detection mechanism using cross-layer and obtained the information from physical and link layer to different between jamming and congested n\w scenarios. To improve the detection accuracy. They utilized the channel utilization metric to evaluate n\w congestion is due to jamming or n\w traffic condition. Through simulation results we demonstrate the effectiveness of our scheme in detecting jamming with improved precision.

[15] Network Intrusion Detection System on Wireless M0bile Ad hoc Networks.

Chilakalapudi Meher Babu et al. In this paper present the IDS on wireless mobile ad-hoc network. The MANET is a infrastructure less. Inside the MANET every node is the centralized controller exist each node contain routing capability, each device freely move any direction in MANET. Is one of the major problem in the wireless MANET face to security? This paper aim is seeing the effects of DDoS in packet dropping, end to end delay, and routing load. This paper inside IDS technique are used to detect the attacker, and to detect the attack and block them. In this paper they are discussed some attacks on MANET and DDoS also and provide the security against DDoS attack. Intrusion detection is the process of monitoring and detecting process and find out the misbehavior node and block it. They proposed security mechanism that block smart n\w from DDoS attack and transport layer attack. This mechanism is clear the unwanted traffic and it is based on the address registration process protocol mechanism the traffic is forwarded from the internet to the smart object network.

## IV. CONCLUSION

Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when come across and maintaining routes for other

nodes in the network. The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Proposed prevention and detection mechanisms will adopt to provide security in ad hoc networks. A precaution-only strategy will only work if the prevention mechanisms are ideal otherwise, someone will find out how to get around them. The proposed scheme will definitely improves the network performance i.e. measured through performance metrics and provides the zero percentage infection after applying the security scheme.

## REFERENCES

[1] Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee ,Aniruddha Bhattacharyya ,Arnab Banerjee , Dipayan Bose "Study Of Different Attacks In Manet With Its Detection & Mitigation Schemes" International Journal of Advanced Engineering Technology IJAET/Vol.III/ Issue I/January-March, 2012/383-388.

[2] Yu-seung Kim, Heejo Lee. On classifying and evaluating the effect of jamming attack.

[3] Alejandro Proan˜o and Loukas Lazos "Packet-Hiding Methods for Preventing Selective Jamming Attacks" IEEE transactions on dependable and secure computing, vol. 9, no. 1, January/February 2012, page(s): 101-114

[4] John Dunlop and Joan Cortes. "Impact of Directional Antennas in Wireless Sensor Networks." In IEEE 2007, p.p.1-6.

[5] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood. "The feasibility of launching and detecting jamming attacks in wireless networks.

[6] Hong Huang "On a New Type of Denial of Service Attack in Wireless Network: The Distributed Jammer Network" IEEE Transaction on Wireless Communication, vol. 10. No. 7, July 2011.page(s): 2316-2324.

[7] Ali Hamieh, Jalel Ben –Othman "Detection of Jamming Attacks in Wireless Ad hoc Networks Using Error Distribution".IEEE ICC 2009" ELSEVIER journal of Network and computer Application, February 2012, page(s) 1-6

[8] Ajana J[1,] Helen K.J[2] "Mitigating inside Jammers in Manet Using Localized Detection Scheme" International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (print): 2319 – 6726 www.ijesi.org Volume 2 issue 7\ July 2013 \ PP.13-19.

[9] Yu Zhang, Loukas Lazos, Member, IEEE, and William Jr.Kozma "AMD: Audit-based misbehavior Detection in wireless Ad Hoc Networks" IEEE transactions on mobile computing, vol. x, no. x, page (s): 1-4.

[10] Mr. Pushphas Chaturvedi, Mr. Kunal Gupta "Detection and Prevention of various types of Jamming Attacks in Wireless Networks" IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.3, No2, April 2013, page(s):75-79.

[11] M. Balakrishnan, H. Huang, R. Asorey-Cacheda, S. Misra, S. Pawar, and Y. Jaradat "Measures and Countermeasures for Null Frequency Jamming of On-Demand Routing Protocols in Wireless Ad Hoc Networks" IEEE transactions on wireless, communication, vol. 11, no. 11, November 2012, page(s): 3860-3868.

[12] Konstantinos Pelechrinis, Christos Koufogiannakis, and Srikanth V. Krishnamurthy, *Member, IEEE* "On the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks" IEEE transactions on wireless, communication, vol. 9, no. 10, October 2010, page(s): 3258-3271.

[13] Jordi Cucurull, Mikael Asplund, Simin Nadjm-Tehrani, Member, IEEE, and Tiziano Santoro "Surviving Attacks in Challenged Networks" IEEE transactions on dependable and secure computing, vol. 9, no.6, November/December 2012, page(s):917-929.

[14] 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, page(s):57-66.

[15] Chilakalapudi, Meher Babu1, Dr. Ujwala, Lanjewar2, Chinta Naga Manisha3, "network Intrusion Detection System on Wireless mobile ad hoc networks" International Journal of Advanced Research in Computer and Communication Engineering Vol l. 2, Issue 3, March 2013, page(s):1495-1500.