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

Mitigating Inside Jammers in Manet Using Localized Detection Scheme

Ajana J.[1], Helen K. J.[2]
[1](*Department of Computer Science, Govt. Engineering College, Thrissur, India)*
[2](*Department of Computer Science, Govt. Engineering College, Thrissur, India)*

ABSTRACT: *Wireless networks have already grown considerably and will certainly go on doing so, consequently the security and secrecy has become a critical issue. To prevent people from communicating with each other, jamming the communication channel is one of the most efficient way and easy to implement. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. The military tactical and other security-sensitive operations are the main applications of ad hoc networks. One type of organization of such a network is clustered approach. But we are using a distributed approach in which the nodes are in promiscuous mode. In this paper, we propose a distributed jamming detection scheme (LDS) in which all the nodes take part in detecting jammer using the basic parameters such as delivery ratio and signal strength. The paper aims to compare this strategy on both type of networks by simulating these using NS2. Simulation results are plotted and analysed. It is observed that the distributed approach is more efficient in detecting jamming attack.***

KEYWORDS: *MANET, ad-hoc network, jamming attack, promiscuous mode, detection.*

I. INTRODUCTION

A wireless computing network is a computing network with no physical cable connected to each other. There are currently two variations of mobile wireless network[2]: the infrastructural network and the Ad-hoc network. An **infrastructural network** is one that extends an existing wired LAN to wireless devices by providing a base station. Each mobile client connects to and communicates with the nearest base station that is within its communication radius. An **Ad-hoc network** is one in which a LAN is created by wireless devices themselves without a fixed base station. The network is peer-to-peer and self-managed. All nodes are capable of movement and can be connected dynamically. Every node can act as, and is ready to act as, a route to an external network at any moment.

A Mobile Ad hoc NETwork (MANET) [2][11] consists of a loosely connected domain of routers. Originally called Mobile Packet Radio, Mobile Ad-hoc Network (MANET) technology has been an important military research area. This technology has practical use whenever a temporary network with no fixed infrastructure is needed. Other uses include rescue operations and sensor networks. The support of these military and civilian uses often requires the presence of a database to store and transmit critical mission information such as inventories and tactical information. There is one other crucial characteristic of a MANET. Traditional mobile networks involve the server in all data communication. MANET includes the traditional database capabilities of data push and data pull, but it also allows the clients to communicate directly with each other without the involvement of the server, unless necessary for routing.

Mobile ad hoc networks (MANETs) are more susceptible to attacks due to the lack of infrastructure. Features such as, open medium, dynamic topological changes, limited bandwidth, distributed cooperation and constrained energy resources are some of the characteristics that make MANETs more vulnerable[7]. The attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks on individual layer are as under[3][7]:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal, External
- Physical: Interference, Traffic Jamming, Eavesdropping

Among these, the focus of this paper is DoS attack in the form of jamming in MANETs. Next section will cover the architecture of MANETs and jamming models as a background information. Section 3 is the literature review in which the related works are discussed. Section 4 describes the proposed localized detection scheme for detecting jamming attacks in MANETs. Section 5 provides a comparison of the performance of the proposed method with the same method implemented in a clustered organization of the nodes. The simulation details and analysis results are also described in this section. Section 6 is the conclusion and future work.

II. BACKGROUND

2.1. Manet architecture and operation

In Fig. 1, a few nodes of a MANET are shown graphically. Each node has an area of influence. This is the area over which its transmissions can be heard. As the power level decreases, the area of influence of any node will shrink. This is due to the fact that the power available to broadcast is reduced. Each node in the network has a number of neighbours, and it maintains a neighbour table which records their information of its neighbours, such as their locations or activeness. Such a neighbour table is maintained by most routing protocols, and it can be easily achieved by periodically broadcasting hello messages[2].

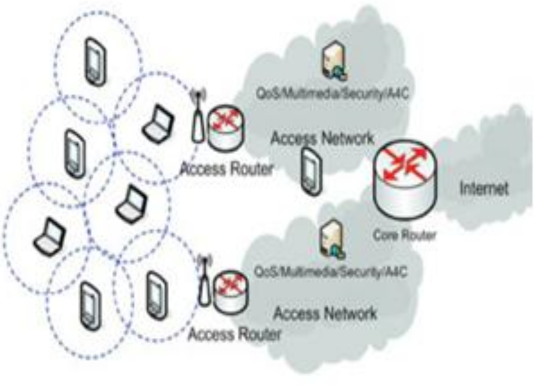

Figure 1: MANET Architecture

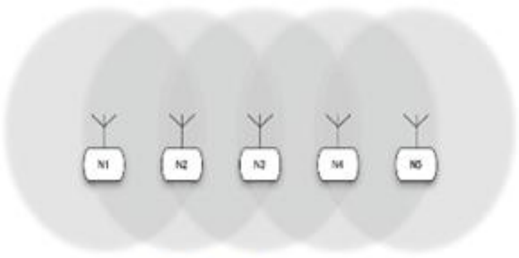

Figure 2: MANET Communication

The nodes in the MANETs also serve as routers with store-and-forward functionalities to achieve multi-hop transmissions. Fig. 2[5] shows a scenario of MANET communication in which there are five nodes. The light grey area indicates the radio coverage area of each MANET interface. N1 and N5, which cannot communicate directly since they are out of radio range from each other, get help from other intermediate nodes for communication.

Two kinds of mobile ad-hoc networks[2][5] can be distinguished.

Mobile ad hoc networks in hostile environments designate a set of mobile nodes that are expected to carry out a mission in an environment where the presence of a “strong” attacker is expected. This is typically the case of military networks. The authority would typically pre-load appropriate cryptographic keys in the devices, in compliance with the role of each of the users; these keys would then protect the communication between the devices during the unfolding of the mission.

In self-organized mobile ad hoc networks, there is no authority whatsoever to take care of the network, not even in the initialization phase. This means that the network is purely peer-to-peer, and that the nodes have to figure out how to secure the communications by themselves. Here, nodes selfishly refuse to forward packets or greedily overuse the common radio channel.

Network nodes may operate in any of three modes that are designed to facilitate the reduction in power used.[5]

- Active Mode (or Transmit Mode): this is the mode using the most power. It allows both the transmission and reception of messages and consumes 3000 to 3400 mW.
- Doze Mode (or Receive Mode): the CPU is capable of processing information and is also capable of receiving notification of messages from other nodes and listening to broadcasts. 1500 to 1700 mW are consumed in this mode.
- Sleep Mode (or Standby Mode): the CPU does no processing and the node has no ability to send/receive messages. The node is inactive and consumes only 150 to 170 mW. This mode allows a node to turn itself off for short periods of time without requiring power-up or re-initialization.
- A node with no remaining power, or one that is off, is not currently a part of the network.

2.2. Jamming Models

A jamming model captures the strategy followed by the malicious attacker. Four jamming models[4] are described in this section. The key attributes of these models lies in their simplicity and effectiveness. A **constant jammer** continually emits radio signals on the wireless medium. The goal of this type of jammer is twofold: (a) lower PDR by corrupting the packets and (b) lower PSR by making the channel busy. A **deceptive jammer** continually injects regular packets on the channel without any gaps between the transmissions. Since the traffics are legitimate, deceptive jamming is difficult to identify. A more power efficient jamming strategy is the use of **random jammer**. A random jammer jams for t_j seconds and then sleeps for t_s seconds. During the jamming intervals, the jammer can follow any of the approaches described above. A smarter and more power efficient approach would be to only target the reception of a packet. This jamming model is called the **reactive jammer**. This jammer is constantly sensing the channel and upon sensing a packet transmission immediately transmits a radio signal in order to cause a collision at the receiver.

In order to quantify the extent to which the jammer satisfies the jamming efficiency criteria, metrics are defined that capture the jammer's behaviour. The following two are the widely used metrics [6][9][10].

Packet Send Ratio (PSR): Assume that the MAC layer of Tx (Transmitter) has n packets for transmission. Due to jamming interference, only m ($n \geq m$) of these packets can eventually be transmitted. PSR is then defined to be[10]:

$$\text{PSR} = \frac{m}{n} = \frac{Packets\ sent}{Packets\ Intended\ to\ be\ sent} \qquad \text{--- (1)}$$

PSR captures the effectiveness of the jammer towards a transmitter employing carrier sensing as its medium access policy. The jamming signals can render the medium busy due to carrier sensing and as a result the transmission queues of Tx will get filled up quickly. Packets arriving at a full queue will be dropped.

Packet Delivery Ratio (PDR): Suppose that Rx receives m packets sent out from Tx . However, from these m packets only q were successfully delivered to the higher layers of Rx (Receiver). A successful reception means that the packet successfully passed the CRC (Cyclic Redundancy Codes) check. In contrast to PSR, PDR captures the effectiveness of the jamming attack towards Rx .The PDR[10] is defined as follows (if m =0 then PDR is defined to be zero):

$$\text{PDR} = \frac{p}{q} = \frac{Packets\ received}{Packets\ sent\ to\ it} \qquad \text{--- (2)}$$

III. RELATED WORKS

Liu in [1] paper addressed the problem of preventing control-channel DoS attacks manifested in the form of jamming. A sophisticated adversary is considered who has knowledge of the protocol specifics and of the cryptographic quantities used to secure network operations. This type of adversary cannot be prevented by anti-jamming techniques that rely on shared secrets, such as spread spectrum. New security metrics are proposed to quantify the ability of the adversary to deny access to the control channel, and introduced a randomized distributed scheme that allows nodes to establish and maintain the control channel in the presence of the jammer. Networks with both static and dynamically allocated spectrum are studied. To mitigate the impact of jamming, a cluster-based architecture is adopted, where the network is partitioned into a set of clusters. Each cluster establishes and dynamically maintains its own control channel. The control-channel establishment and maintenance process is facilitated by a cluster head (CH) node within each cluster. CHs are regular nodes that are temporarily assigned with the responsibility of mitigating jamming, and can be periodically rotated. Two algorithms are proposed for unique identification of the set of compromised nodes, one for independently acting nodes and one for colluding nodes. Detailed theoretical evaluation of the security metrics and extensive simulation results are provided to demonstrate the efficiency of the methods in mitigating jamming and identifying compromised nodes.

Gagandeep in [2] discussed various types of attacks on various layers under protocol stack. Different types of attacker attempts different approaches to decrease the network performance, throughput. Routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication are also described. On the basis of the nature of attack interaction, the attacks against MANET may be classified into active and passive attacks. Attackers against a network can be classified into two groups: insider and outsider. An outsider attacker is not a legitimate user of the network, whereas an insider attacker is an authorized node and a part of the routing mechanism on MANETs.

Ali in [3] considers jamming attacks in wireless ad hoc networks. It describes in detail about various types of jammers that can be present in the network. The also proposed an approach of Jamming Detection which is based on the measure of statistical correlation among the periods of error and correct reception times. They assume that the jammer transmits only when a valid radio activity is signalled from its radio hardware. The dependence measure in jamming attack case is greater than in normal network activity. NS-2 is used to evaluate the correctness of the detection system.

Le in [4] described in detail about jamming attack types and a combined approach to distinguish them. Based on the shared characteristics of the wireless medium, a wireless network can be easily affected by jamming attacks, which is one of the most effective forms of denial-of- service (DoS) attacks against this type of networking architecture. Attacks can be implemented by either corrupting the operations of the medium access control (MAC) protocols or transmitting large amounts of interfering wireless signals without obeying the MAC protocols. Most jamming detection approaches cannot provide an effective way for differentiating between the various categories of jamming attacks. To enable the network to perform defense strategies more effectively, distinguishing the type of different jamming attacks is necessary. The paper distinguishes different types of jamming attacks using a statistical model based on Packets Send Ratio (PSR) and Packets Delivery Ratio (PDR) in different jamming situations. After knowing the exact type of jamming attacks, the nodes can implement a more efficient method to defend jammers. The evaluation of the proposed strategy was done in ns-2 simulation platform.

In the work by Kaur[8], jamming attack is introduced in the networks having nodes with isotropic and directional antennas. It includes a study of different types of jammers and antenna patterns. The proposed method using antennas are implemented using OPNET modeller. Bit Error Rate, Packet Loss Ratio, SNR, Throughput and Utilization are taken as performance evaluation parameters. The simulation results show that it is possible to minimize the effect of jamming attack by using different antenna patterns.

IV. LOCALIZED DETECTION SCHEME FOR JAMMING ATTACKS

The traditional spread spectrum techniques rely on the fact that the hopping sequence or PN code is shared among the users in the network. If the jammer is a member of the network, the secret code is known to him and can intelligently jam the channels. So spread spectrum techniques are not suitable for preventing internal jamming attack. As proposed by Liu et al [1], cluster based architecture can be used. Each cluster will have a cluster head (CH). It is the responsibility of the CH to generate unique hopping sequence for all the cluster nodes and detect jamming attack. Such a centralized approach is not desirable in an ad-hoc environment. So we suggest a distributed approach in which all the nodes monitor every other node in its neighbourhood. The nodes are said to be promiscuous mode of operation. If it found some malicious behaviour from any of its neighbour, the node will broadcast an alert indicating the existence of a suspected node in the network. Signal strength (SS) and PDR can be used to find out the misbehaved node[9]. The algorithm for detecting the jammer in the network is shown in Fig. 3.

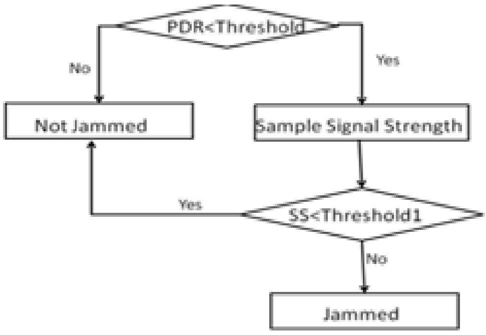

Figure 3: Algorithm for jammer detection

One problem that may arise in this method is a false alarm. That is, a jammer can send a false message indicating any other node as a jammer. To avoid this problem, reputation of the nodes must be kept in track. Reputation is computed as a measure credibility of a node. When a node is compromised, its only job will be disrupting the communication by sending unnecessary signals through the channels. So it won't spend energy in forwarding the packets. Reputation is the ratio of number of packets forwarded to number of packets sent. For a compromised node, the value of reputation will be very low. Message from such nodes regarding other nodes will not take as valid. Once a jammer is detected, it must be isolated from the network by not sharing any of the secret code and messages with it.

V. SIMULATION SETUP AND RESULTS

The simulation of the proposed method is done using ns-2[12], an open-source event-driven simulator for both wired and wireless networks. NS2 provides users with an executable command ns which takes on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. Simulation parameters are :

1) Grid size : 200 by 200 meters
2) Number of nodes : 10, 20, 50 mobile nodes (number of nodes varied)
3) Packet Traffic : CBR
4) Mobility : Random Way Point mobility model
5) Routing Protocol : AODV
6) MAC Layer : 802.11, peer-to-peer mode.
7) Radio : “no fading” radio model, with range of 376 meters.
8) Antenna : Omni-directional with unity gain
9) Simulation Time : 200 sec.

The proposed method is implemented in the MAC layer of the 802.11 protocol in ns2. The simulation proceeds as follows. First, we simulated a network with 10 nodes organized into two clusters. Each cluster has a cluster head. It will periodically check the network for malicious behaviour. When one of the node in its neighbourhood act as a jammer, the cluster head identifies that node and broadcast a message to all the cluster nodes indicating the identity of the jammer node. Then the neighbours will isolate the jammer node by denying service to it. The simulation is then extended for 20 and 50 nodes with number of clusters increased accordingly. Delivery ratio, overhead and energy consumed by the nodes are analysed. The same scenario is simulated with our localize detection scheme (LDS). From the simulation results, it is evident that LDS is better than the clustered approach.

5.1. Performance comparison using delivery ratio

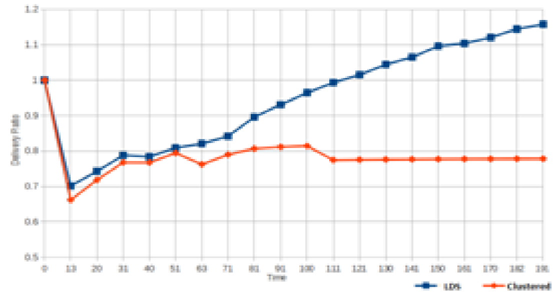

Figure 4(a): Delivery ratio with 10 nodes

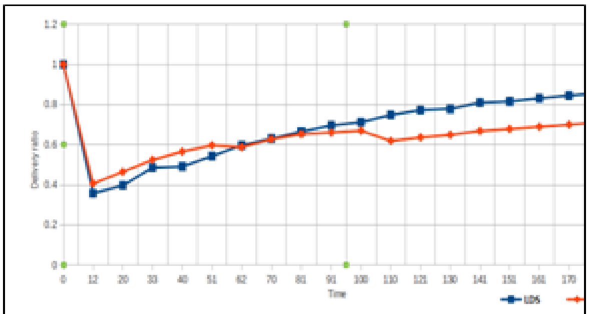

Figure 4(b): Delivery ratio with 20 nodes

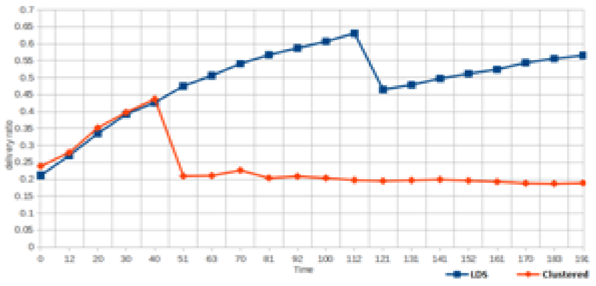

Figure 4(c): Delivery ratio with 50 nodes

Fig. 4(a), 4(b) and 4(c) shows the graph of delivery ratio plotted from the result of the simulation of LDS and clustered approach with 10, 20 and 50 nodes respectively. In the 10 node network, the delivery ratio of LDS is more than clustered approach before and after the jammer activity which is scheduled to occur from 50 seconds. In the 20 nodes and 50 nodes network, till the beginning of the jammer activity, clustered approach shows greater delivery ratio. But during the jammer activity, LDS shows high performance. This implies that LDS can successfully deliver the packets in the presence of jammer by faster detection nd isolation of it from the network.

5.2. Performance comparison using overhead

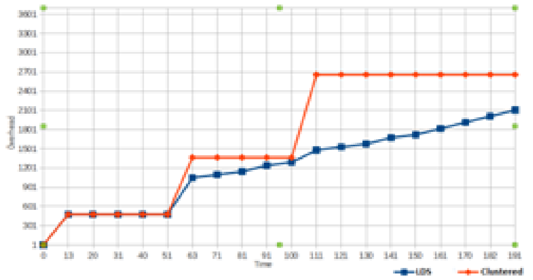

Figure 5(a): Overhead with 10 nodes

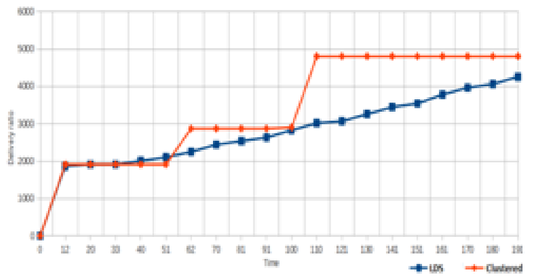

Figure 5(b): Overhead with 20 nodes

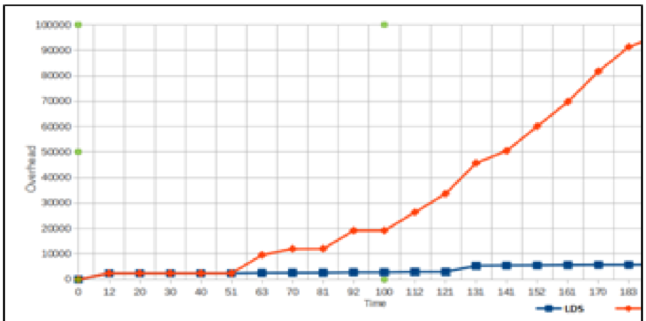

Figure 5(c): Overhead with 50 nodes

Figure 5(a), 5(b) and 5(c) shows the overhead of LDS with clustered approach. Overhead of the clustered approach is more than LDS. As you can see, in a 50 node network, the overhead of the clustered approach is drastically high after the occurrence of jamming activity. This is due to the resending of the packets when undelivered due to jamming attack.

5.3. Performance comparison using energy

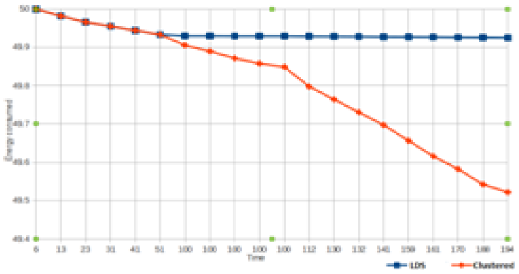

Figure 6(a): Energy consumption of a node in 10 node network

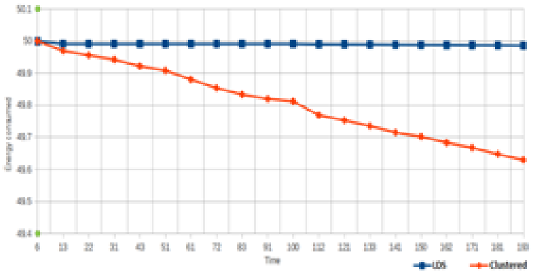

Figure 6(b): Energy consumption of a node in 20

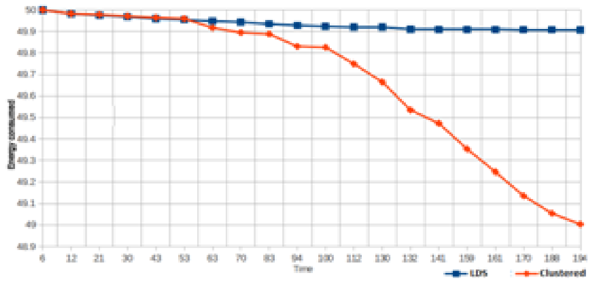

Figure 6(c): Energy consumption of a node in 50 node network

Figure 6(a), 6(b) and 6(c) are the energy consumed by one of the node in 10, 20 and 50 node network. For the purpose of simulation, the energy of the mobile nodes are initially set to 50mW. Once the network is initialized, the nodes began utilizing energy for transmission, reception and also broadcasting of messages. In the clustered approach, the nodes consume more energy than the LDS. Even in the presence of jamming activity, LDS shows a stable use of energy.

VI. CONCLUSION

Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. The proposed method will act as a localized detection scheme(LDS) for identifying inside jammers in the MANET. The research compares the performance of LDS and a cluster organized network. Jamming attack mitigation and detection in the ad-hoc network using the algorithm by using delivery ratio and signal strength is less efficient in clustered organization. Delivery ratio,overhead and energy are used as performance evaluation metrics. Even though managing the reputation values creates a little overhead, it is actually there along with some of the routing protocols. By mitigating jamming attacks, bandwidth utilization can be improved and hence improving the overall network efficiency.

The work can be extended to include some new, more refined metrics for measuring the efficiency of the jamming attack and also for finding the type of jammer. If we can find the type of the jammer, suitable mechanisms can be formulated for their identification and isolation.

REFERENCES

[1]. Sisi Liu, Loukas Lazos, and Marwan Krunz, “Thwarting Control-Channel Jamming Attacks from Inside Jammers,” IEEE Transactions on mobile computing, vol. 11, pp. 1545–1558, September 2012

[2]. Levente Buttyan and Jean-Pierre Hubuax, Security and cooperation in wireless networks- Thwarting Malicious and Selfish Behavior in the age of Ubiquitous Computing, A graduate text book, version 1.5.1, July 27, 2007

[3]. Ali Hamieh and Jalel Ben-Othman, “Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution,” proc. IEEE ICC 2009

[4]. Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, “Denial of Service Attacks in Wireless Networks: The Case of Jammers,” IEEE Communications Surveys & Tutorials, vol. 13, no. 2, second quarter 2011

[5]. Leslie D. Fife, Le Gruenwald, “Research Issues for Data Communication in Mobile Ad-Hoc Network Database Systems,” unpublished.

[6]. Sangwon Hyun, Peng Ning and An Liu, “Mitigating Wireless Jamming Attacks via Channel Migration,” 31st International Conference on Distributed Computing Systems Workshops’11

[7]. Gagandeep, Aashima and Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack- A Review,” International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, Vol.1(5), June 2012

[8]. Tajinderjit Kaur and Sangeeta Sharma, “Mitigating the Impact of Jamming Attack by Using Antenna Patterns in MANET”, VSRD-IJCSIT, Vol.2 (6), pp. 437-445, 2012

[9]. Le Wang and Alexander M.Wyglinski, “A combined approach for distinguishing different types of jamming attacks against wireless networks”, proc. In Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference, pp. 809-814.

[10]. Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, MobiHoc '05 Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57.

[11]. David J. Thuente and Mithun Acharya, “Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks”, MILCOM'06 Proceedings of the 2006 IEEE conference on Military communications, pp. 1075-1081

[12]. Teerawat Issariyakul and Ekram Hossain, Introduction to Network Simulator NS2 (Springer)