# Literature Survey on Jamming Attack in Wireless Adhoc Network

Pinal Rupani
Computer Engineering Department
V.V.P. Engineering College, Rajkot
Gujarat, India

Prof. Naren Tada
Computer Engineering Department
V.V.P. Engineering College, Rajkot
Gujarat, India

***Abstract*** **-** Wireless Adhoc Network is a set of wireless nodes which dynamically self-organizing into an changeable topology to form the network using any preceding infrastructure. The number of nodes present in the network either communicate directly with each other or in case if it do not communicate directly, just communicate by forwarding traffic through intermediate nodes. Each adhoc nodes acts as a router. Wireless Infrastructure network are highly affected by various attacks such as Blackhole, Grayhole, Wormhole, Jamming attack, etc. This paper gives survey of jamming attack. These types of attacks can undoubtedly be accomplished by an opponent either by passing MAC layer protocol or sending Radio Signals. Reviewing the role of wireless adversary, which victims the packets of high importance and do not follow network architecture. Attacker will make possible efforts of making users not to use network resources and fail the communication. This paper presents an overview of Jamming attack in wireless adhoc network and prevention techniques to get secure from severe jamming effect. It has been surveyed that using NS-3, Jamming attack can be recognized through increase of energy consumption.

***Index Terms*** **-** MANET, Jamming attack, Categorization of Jammer, Localization of jammer, Prevention Techniques, NS-3 Jamming Module and Energy Model

## I. INTRODUCTION

WIRELESS SECURITY is the most critical attributes of Wireless communication. Wireless Adhoc Network[1] are continuously enhancing towards miscellaneous attacks and achieving ubiquitous computing. Mobile Adhoc Network (MANET)[4,8,10] is dynamic, independent, multi-hop network. MANET does not be in need of any fixed framework and it can be installed dynamically. Due to existence of multi-hop nature in MANET, lots of vulnerabilities present in the network. As these networks furnishing more security or more comfort zone, the issue of critical importance also come up. In MANET, different attacks such as, DDOS, Blackhole, Wormhole, Replay, Flooding, Jamming,[2,4,10] etc have been perceived, which results in adverse effect of high-level security. Since owing to fact that, Security in MANET[10] is becoming challenging day by day. Attacker easily view the wireless communication between two devices and initiate simple Denial-of-Service attack against wireless network by placing distorted messages.

Radio interference attacks don't seem to be available through conventional security mechanisms. An attacker will merely disregard the medium access protocol and frequently transmit on a wireless channel. On doing so, we can either intercept users to start up with legitimate MAC operations, or found packet collisions that force repeated back-offs or also jams communications.

The main aim of this paper is to give summary of important issue of Jamming in wireless adhoc network

and cover all the related work. Following fig.1 shows the pictorial view of Jamming attack.

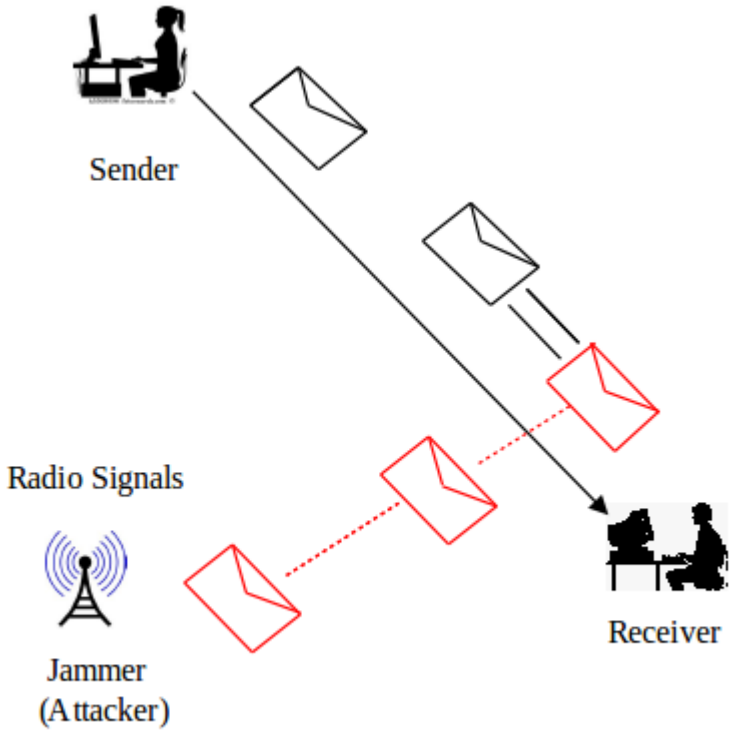



**Fig.1** Jamming Attack

To know how jammer attacking in wireless networks and how to stay away from this jamming, researchers launch three aspects: 1. Types of existing jammers, 2. Protocols for localizing jammer and, 3. Detection and Prevention techniques. The flow of this write-up is ordered as follows: Section I incorporate an introduction to main concept and issues of MANET, Section II gives overview of Jamming Techniques, Section III gives overview of NS-3 Jamming Module and Energy Module.

## II. RELATED WORK

### *2.1 Jamming Efficiency Metrics:*

Jamming efficiency criteria includes

- Energy efficiency
- Probability of Detection
- Level of DoS
- Strength against physical layer techniques

Jamming attack should consume low power, low possibility of detection (ideally close to 0) and disrupt communication upto maximum possible extent. This is severe attack that do not permit signal processing technique to overwhelm the attack. To fulfill above standards, researchers defined few metrics that apprehend the jammer's activity. Consider the situation with one Sender(Sx) and Receiver (Rx).

Xu et al [5] found two metrics (PSR and PDR).

*1. Packet Send Ratio (PSR):* [5,6]

In this article, let us acquire that ***n*** number of packets transmitting through channel. Only ***m*** **(*n>=m*)** of these packets transmitted correctly.

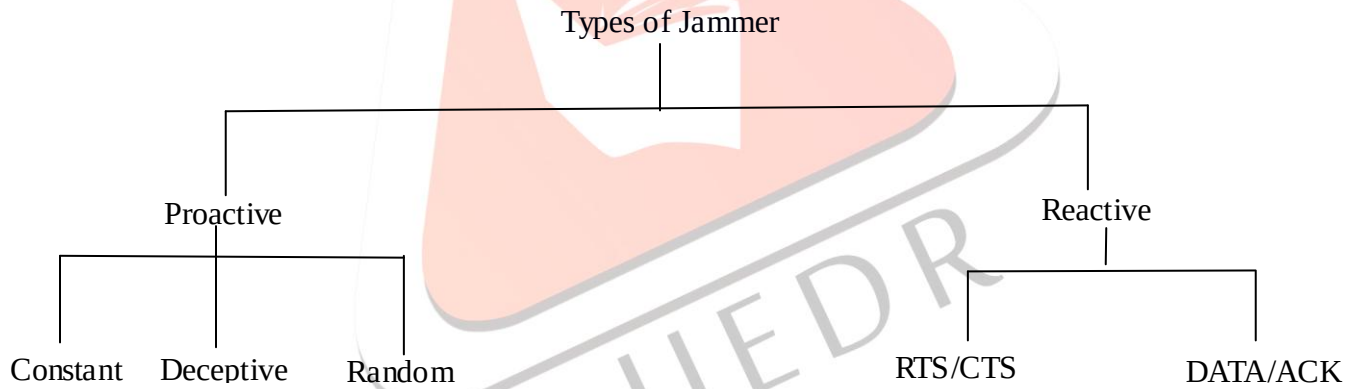
$$PSR = \frac{m}{n} = \frac{\text{No. of Packets Sent}}{\text{Packets Observed to be Sent}} \quad \text{.} \quad \text{....[i]}$$

***2.*** *Packet Delivery Ratio (PDR):* [5,6,7,9]

Lets acquire that Rx receive m packets sent from Sx. But unfortunately only q of packets broadcast successfully to Rx. Packets proceed from CRC (Cyclic Redundancy Codes) check are reffered as successful acceptance of Packets. If m=0, then PDR be zero.

$$PDR = \frac{q}{n} = \frac{\text{Packets undergo CRC}}{\text{No. of Packets Received}} \quad \text{..... [ii]}$$

***2.2 Types of Jammer:***




**1) Proactive Jammer:**

Proactive Jammers[7] initiate to disrupt channels by imparting Jamming signals without assuring whether there is data communication in network or not. The channel whose status is on, it dispatch packets or random bits onto that channel.

*[i] Constant Jammer: [6-9]*

A constant jammer persistently producing radio signals on wireless channel. The purpose of this type of jammer is dual: (a) to raise interference on any of the transmitting node in a way to distort its packets at the receiver (lower PDR) and (b) to form a authorized sender that (by using carrier sensing mechanism) sense the channel busy, thus preventing it from acquiring access to the channel (lower PSR).

*[ii] Deceptive Jammer: [6-9]*

Persistently dispatching normal packets instead of transmitting random bits (during the time of constant jammer). It misguides other nodes to assume that some genuine activity going on. As a consequence they continue to exist in receiving states upto the time the jammer is turned off or dies. Alike to the constant jammer, deceptive jammer is energy ineffectual because of the constant transmission, but is straightforwardly executed.

*[iii] Random Jammer:* [6-9]

This Jammer periodically send either random bits or normal packets into network. Conflicting to the above two jammers, it targets to save energy. It constantly moving by linking two states: sleep and jamming phase. It sleeps for a certain amount of time and then comes in a operative/ working mode for jamming before it go back to a sleep state. The sleeping and jamming time periods are either fixed or random. There is a trade-off between jamming effectiveness and energy saving as it can't be jammed at the time of its sleeping phase. The ratios between both phase can be handled to regulate this trade-off between efficiency and effectiveness.

**2) Reactive Jammer:**

Reactive jammers go ahead for jamming only when it discover some network activity arise on a few channel. It can distort small and large sized packets. Afterall it has to repeatedly watchdog the network, as reactive jammer is less energy efficient than random jammer. Upcoming are two different techniques to implement a reactive jammer.

*[i] RTS/CTS:* [7]

Jams the network as soon as it get aware that a request-to-send (RTS) message is transferred from a sender, it begins to jam the channel. In this way, the receiver will not send back clear-to-send (CTS) response as the RTS packet sent from a sender is distorted. Then, the sender will not send data as it imagines that the receiver is engaged with another on-going transmission. Alternatively, the jammer can standby after the RTS to be received and jams when the CTS is sent by the receiver which result in the sender not sending data and the receiver always waiting for the data packet.

*[ii] DATA/ACK:* [7]

Jams the network by altering the transmissions of data or acknowledgement (ACK) packets. It don't react till the data transmission begins at the transmitter end. This jammer can suborn data packets, or it standby upto the time, the data packets reach the receiver and then corrupts the ACK packets. The alteration of both packets shows re-transmissions at the sender end. Earlier, there was case where data packets were not able to receive it precisely, they have to be retransmitted. Later on, since the sender don't receive ACK packets, it imagine that something is wrong at receiver side, as in case of buffer overflow, which again results in re-transmission of data packets.

### 2.3 Types of Jamming:

*[i] Physical Jamming: [11]*

Physical in a wireless environment is a effortless however it troubled different form of Denial-of-Service attack. These attacks are caused by either repeatedly transmitting radio signals or by dispatching random bits onto the channel. Different types of jammers cause severe attacks (i.e. Jamming Attack) can contradict complete access to the channel by controlling the wireless environment. This makes each node to wait for certain amount of unusual carrier sensing time[5] till the channel become idle to communicate. Thus, there is an unfortunate effect as all the nodes passed into the exponential back-off periods.

*[ii] Virtual Jamming: [11]*

Virtual carrier sensing mechanism used at the MAC (Media Access Control) layer. In IEEE 802.11 based MAC protocols, virtual jamming play a vital role in determining the presence of the wireless medium. In MAC layer, the effect of Jamming begins by attacking on the RTS/CTS frames or DATA/ACK frames. We realize some notable benefits of MAC layer jamming that rival nodes utilize less power in targeting severe attacks compared to the physical jamming.

### 2.4 Jamming Model:

When messages start getting corrupted due to jamming attack, this model decided to split the entire network nodes into three groups as soon as network start affecting from jamming effect. Three groups are basically named as Jammed nodes, Boundary nodes and Unchanged nodes.

Jammed nodes is located inside the jammed part of network and ultimately it cannot receive packets from any of its neighbors. Boundary nodes are those nodes which are located at the edge of jammed region, is not jammed but part of its neighbors are jammed. Unchanged nodes are those nodes which are located outside the jammed region and it don't get changed or affect from jamming.

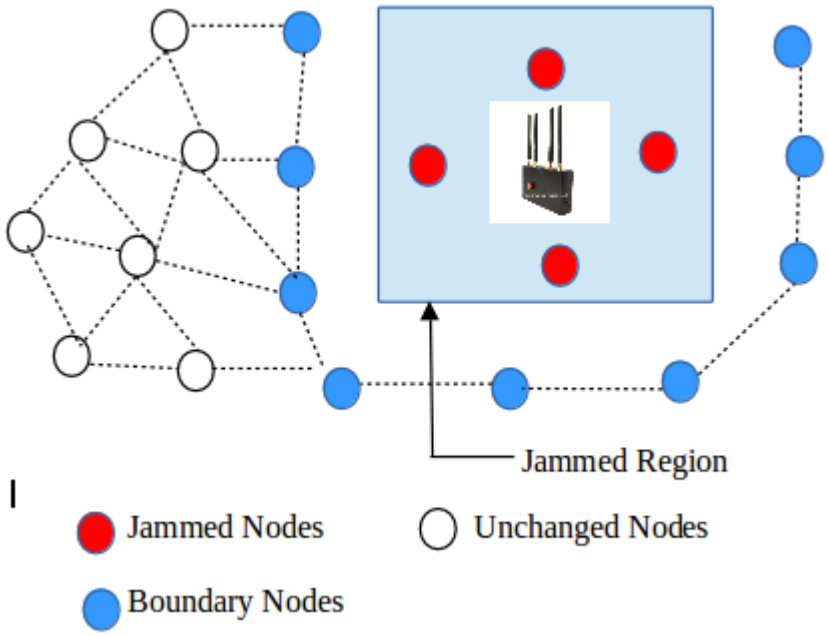



**Fig.3** Graphical View of Jamming Module

## 2.5 Protocols for localizing Jammer:

*[i] Centroid Localization (CL):*

Centroid based scheme [7,12] is useful in localizing the jammer's position. The main advantage of the protocol is that it conduct the estimation without collaborating with target nodes. First CL collects the information regarding the position of all the neighboring nodes which are placed inside the transmission range of target node. As per the jamming model, the neighboring nodes of jammer are "Jammed Nodes". Thus to determine the jammer's position, CL fetch all coordinates of jammed nodes and averages it over their coordinates.

*[ii] Weighted Centroid Localization (WCL):*

WCL[12] is a further step of CL to improve the results by producing better estimation. In this method, we guess the position of jammer by evaluating the weighted average. This algorithm uses an metric called "Weight" which is the distance between jammer and jammed nodes. Since we are not aware about how much transmission power is needed and thus it is difficult to distance between jammer and jammed nodes. The feasible way to obtain the distance is to compute the RSS (Received Signal Strength) of the incoming signal.

## 2.6 Jamming Prevention Technique:

*[i] Virtual Force Iterative Localization (VFIL):* [7,12,13]

VFIL came into picture for achieving better precision than WCL and free from RSS readings. To represent this algorithm, two virtual forces are defined i.e. F-pull initiate by jammed nodes outside the jammed region and F-push initiate by boundary nodes which are placed inside the jammed part. Assume,

(X1, Y1) – estimated place of jammer's
(Xm, Ym) – place of jammed node
(Xj, Yj) – site of boundary node

$$\text{F-pull} = \frac{Xm-X1}{\sqrt{(Xm-X1)^2+(Ym-Y1)^2}}, \frac{Ym-Y1}{\sqrt{(Xm-X1)^2+(Ym-Y1)^2}}$$

$$\text{F-push} = \frac{X1-Xj}{\sqrt{(X1-Xj)^2+(Y1-Yj)^2}}, \frac{Y1-Yj}{\sqrt{(X1-Xj)^2+(Y1-Yj)^2}}$$

$$\text{F-joint} = \frac{\sum m\varepsilon J \ \text{F-Pull} + \sum j\varepsilon B \ \text{F-Push}}{\left|\sum m\varepsilon J \ \text{F-Pull} + \sum j\varepsilon B \ \text{F-Push}\right|}$$

**ALGORITHM:** [12,13]

**Step 0:** Detect the jamming attacker

**Step 1:** Estimate the position of the jammer. The initial estimation is obtained by calculating the Centroid of all jammed nodes.

**Step 2:** Derive the estimated jammed part, which is circle centered with the radius same as jammed region.

**Step 3:** Derive F-pull and F-push using above methods, and form the joint force i.e F-joint.

**Step 4:** Set an adjustable moving step, and move the estimated jammer's position along the direction of F-joint to a new estimate position.

*[ii] Honeypots:* [14]

Honeypots are essentially security mechanism used to preventing from jamming attack. In this technique, basically honeypot are specific nodes which is used to divert the focus of attacker present in the network. The primary function of honeypot is to gain attention of attacker by confining them in a way that attacker will try to attack on honeypot node by thinking that it is dominant area of network. Simultaneously, honeypot will accumulate all the data of attacker like his strategy and purpose. Honeypots are the efficient way for handling jamming attack in wireless infrastructure network.

**ALGORITHM:** [14]

**Step 1:** Scan the current channels to detect the presence of jammer.

**Step 2:** If honeynode detects the attack

- It immediately informs the base station.
- It continues to communicate with jammer to waste time.
- The base station informs the associated mobile nodes to change the channel of operation.
- The mobile node gets the next channel using pseudo random sequence.

**Step 3:** If base station detects the attack

- Inform the honeynode about attack.
- Send information to associated nodes.
- If the nodes send response to the base station, then the base station issues a frequency.
- If any of node don't response, the base station broadcast frequency change command and change frequency of operation.

**Step 4:** If mobile nodes detects the attack

- Wait to receive information from base station.
- If information not received within the time limit, choose the next channel using pseudo random sequence.

## III.NS-3 JAMMING MODULE AND ENERGY MODEL

This wireless jamming module*[16]* previously implemented in NS-3 and available at www.nsnam.org. Network get affected by Jamming through continuous emission of radio signals which disrupts the legitimate communication by decreasing several performance metrics such as signal-to-noise(SNR), PDR or PSR values.

It has been surveyed that jamming attack can be recognized by increase of energy consumption. NS-3 also provides Energy Model*[16]* which is the main part for the simulation. Energy model in NS-3 works by collecting data in the form of power emission which can be increased or decreased at each node due to interference caused by jammer's. Wu et al. (2011) provides power equation to estimate data transmission power,

$$E_i + 1 = E_i + V \times (t_{i+1} - t_i) \times I_i$$

where,

$E_i$ = Energy Consumption
$t_i$ = Time Stamp
V = Supply Voltage

Energy Model involves two main components:

*1. Energy Source:*

This class provides basic functionalities such as maintain record of total energy consumption, remaining energy, etc. Single energy source will survive on a node, which shows the total amount of reserved energy at the node.

*2. Device Energy Model:*

This base class monitors the state of each multiple device, calculate and maintain record of total energy consumption of device.

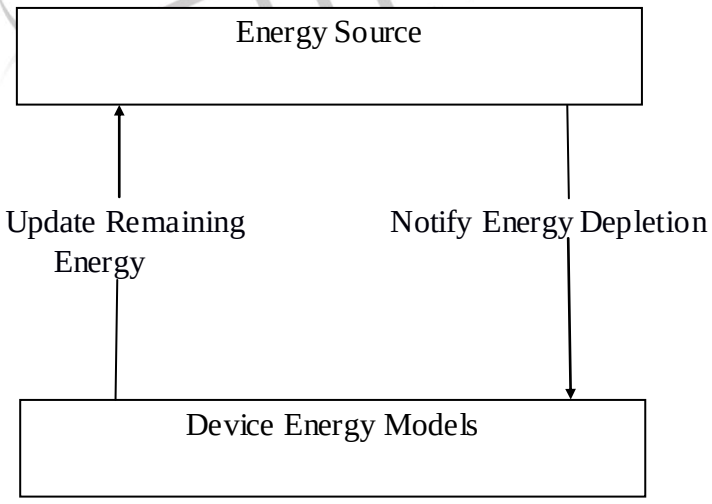



**Fig.3** Energy Model Information Flow*[16,17]*

Fig. 4 shows that Jamming Module successfully integrated in NS-3. [17]

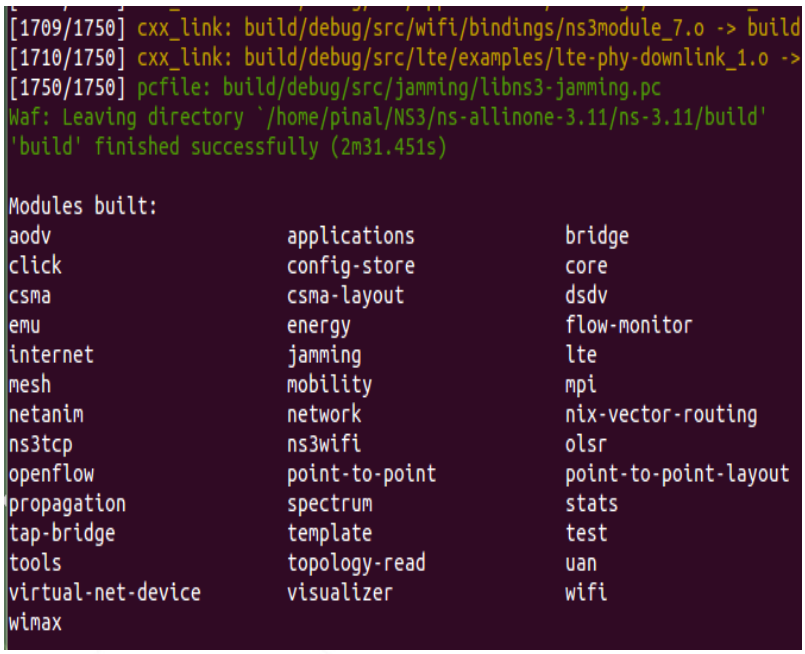



**Fig.4** Build Jamming Module

## IV. CONCLUSION

By studying a lot on jamming attack, we are summarizing various approaches and discussed the severe effect of jamming attack in the wireless network. It has been viewed in our survey that using carrier sensing time or PDR individually, one is not able to conclude the existence of jammer in network. Various prevention techniques are available but to detect jamming attack is very difficult currently. Several issues is addressed such as: 1) Detection of energy efficient scheme 2) Category of detected jammer. Furthermore, it is hard to prevent this types of attacks due to nodes mobility .

## REFERENCES

1. Marcelo G. Rubinstein, Igor M. Moraes, Miguel Elias M. Campista, Luis Henrique M. K. Costa, and Otto Carlos M. B. Duarte, “A survey on Wireless Adhoc Network” , in Springer , 2006.

2. Tada Naren, Patalia Tejas and Patel Chirag, “Trust Appraisal Based Neighbor Defense Secure Routing to Mitigate Various Attacks in Most Vulnerable Wireless Adhoc Network”, in Springer International Publishing Switzerland, 2016

3. Savita Gandhi SMIEEE1 , Nirbhay Chaubey MIEEE2 , Naren Tada3 , Srushti Trivedi3, “Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET”, in IEEE, Jan. 10 – 12, 2012

4. BOUNPADITH K ANNHAVONG, HIDEHISA NAKAYAMA , YOSHIAKI NEMOTO, AND NEI KATO, “A survey of Routing Protocols in Mobile Adhoc Network”, in IEEE, October 2007.

5. Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, in Wireless Information Network Laboratory (WINLAB), Rutgers University, 73 Brett Rd., Piscataway, NJ 08854, 2005

6. Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, “Denial of Service Attacks in Wireless Networks: The Case of Jammers”, in IEEE, VOL. 13, NO. 2, SECOND QUARTER 2011

7. K Grover, "Jamming in Wireless Networks: A Survey", in Int. J. Ad Hoc and Ubiquitous Computing, Vol. x, No. x, xxxx, 2014

8. Ali Hamieh, Jalel Ben-Othman CNRS-PRiSM Laboratory, University of Versailles 45 av. des Etats Unis, 78035 Versailles, France, "Detection of Jamming Attacks in Wireless AdHoc Networks using Error Distribution", in IEEE, 2009

9. Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang, Rutgers University, "Jamming Sensor Networks: Attack and Defense Strategies", in IEEE Volume:20, Issue: 3, May-June 2006

10. Rui Zhang, Jingchao Sun, Yanchao Zhang, and Xiaoxia Huang, "Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks", in IEEE, Oct 8 2015

11. Mr. Pushphas Chaturvedi Mr. Kunal Gupta, "Detection and Prevention of various types of Jamming Attacks in Wireless Networks", in IRACST, Vol.3, No2, April 2013

12. Hongbo Liu, Wenyuan Xu, Yingying Chen, Zhenhua Liu, "Localizing Jammers in Wireless Networks", in IEEE, 2009

13. Hongbo Liu, Zhenhua Liu, Yingying Chen, Wenyuan Xu, "Determining the position of a jammer using a virtual-force iterative approach", in Springer, 23 October 2010

14. Sudip Misra, Sanjay K. Dhurandher, Avanish Rayankula, Deepansh Agrawal, "Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks", in ELSEVEIR, 12 May 2009

15. Neha Thakur, Aruna Sankaralingam, "Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks", in IRACST, Vol. 3, No.2, April 2013

16. Nur Cahyono Kushardianto, Yudhi Kusnanto, Elvian Syafrurizal, Ahmad Hamim Tohari, "THE EFFECT OF JAMMING ATTACK DETECTION AND MITIGATION ON ENERGY POWER CONSUMPTION (CASE STUDY IEEE 802.11 WIRELESS ADHOC NETWORK), in Journal Teknologi, 25th November 2015

17. Network Security Lab, University of Washington (2012, May 10). NS-3 wireless jamming model [Online]. Available: http://www.nsnam.org/wiki/index.php/NS3_wireless_jamming_model.