Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Comparative Evolution of With and Without Jamming Attack in MANET

[1]Baljinder Singh, [2]Dinesh Kumar
[1]Student Masters of Technology Department of CSE, GZS-PTU Campus, Bathinda, Punjab, India
[2]Assistant Professor, Department of CSE, GZS-PTU Campus, Bathinda, Punjab, India

***Abstract-- A MANET is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. WSN's are being used in many applications like automation of home i.e. like centralized control of lights, HVAC (heating, ventilation and air conditioning), appliances, security locks of gates and doors and other systems, to provide improved convenience, comfort, energy efficiency and security and other example is area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines and other examples includes health care, forest fire detection, landslide detection, water quality improving and many more. Hence, their security is critical issue. They are more vulnerable to attacks than wired networks. Wireless sensor networks suffer from various active and passive attacks. Jamming attack is one of them in which signal is totally jammed for the entire network. This paper mainly deals with the security issues and effect of Jamming attack on Ad-hoc network. In Ad-hoc network, active attack i.e. DDOS, black hole attack, wormhole attack, jamming attack can easily occur. These attacks can decrease the performance of the communications protocol. The given paper gives the comprehensive analysis and comparison of the effect of with and without Jamming attack and its features in proposed routing protocol IAODV. In this paper, the analysis of with and without Jamming attack performed on the proposed routing protocol IAODV on different parameters namely throughput and packet delivery ratio. The results of throughput and packet delivery ratio for isolation of attack is quiet better and optimist as compare to the with Jamming attack scenario.***

***Keywords---Mobile Ad Hoc Network; AODV Protocol; Jamming Attack; Wireless sensor networks***

## I. INTRODUCTION

Wireless networks have paved the way for mobile nodes to communicate with each other. The two basic system models are fixed backbone wireless system and wireless Mobile Ad hoc Network (MANET).[1] A MANET is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. Therefore the functioning of ad hoc networks is dependent on the co-operation of each and every node.[4][8] The nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. The rapid proliferation of wireless ad-hoc networks and mobile computing applications has changed the landscape of network security. Wireless networks are networks which provide users with connectivity regardless of their actual physical location. [5]WSN's (Wireless sensor Networks) are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment.

### *Jamming Attack*

It is a type of DOS attack. There are many different attack strategies that a jammer can perform order to interfere with other wireless communications. Some possible strategies are exposed below:

• Constant Jammer: A constant jammer continuously emits radio signal that represents random bits; the signal generator does not follow any MAC protocol.

• Deceptive Jammer: Different from the continuous jammers, deceptive jammers do not transmit random bits instead they transmit semi-valid packets. This means that the packet header is valid but the payload is useless. [2]

• Random Jammer: Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second mode (the 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: A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify as many bits as possible given that only a minimum amount of power is required to modify enough bits so that when a checksum is performed over that packet at the receiver it will be classified as not valid and therefore discarded. [12][14].

## II. RELATED WORK

Bo Yu, Lu-yong Zhang (2014) [3] worked over an improved detection method for different types of jamming attacks in wireless networks. In this paper, a detection method was improved for different types of jamming attacks in wireless

 

networks. Based on the open nature of wireless networks, wireless networks were susceptible to jamming attacks. Most detection methods could not provide effective protection against different types of jamming attacks. In order to effectively improve the defense capability of the wireless network, to identify the precise type of network attack was quite necessary. First, the author roughly classified the types of jamming attacks by existing detection methods. Then based on the statistics of Packet Send Rate (PSR) and Packet Delivery Rate (PDR), they improved the existing detection mechanism and further precisely identify the specific type of jamming attacks when using different types of MAC protocols. Finally, this detection mechanism was simulated by ns-2 simulation platform and the result was quiet optimist and authentic.

G.Mahalakshmi,Dr.P.Subathra (2014)[6] proposed a survey on prevention approaches for denial of sleep attacks in Wireless Networks in which different approaches for the detection of denial of sleep attacks in WSN were described . In this approach , the expected absorption time of sensor network was examined which denoted the Network the lifetime and , finally they concluded that in the survey of various methods and technique such as AMC model, cross layer security mechanism , ITIDS , storm control mechanism , art based routing algorithm required large scale alteration required and were unrealistic so there must be need of some more technique for prevention of denial of sleep attacks which might be performed with minimum changes, cost and resources.

Hong Huang, Nihal Ahmed, and Pappu Karthik(2011)[10], In this paper, the author introduced a new type of denial of service attack to wireless networks: distributed jammer network (DJN), which was made of a large number of low-power, tiny radio jammers. Recent advancements in MEMS and NANO technologies made it possible to build nano-scale jammers that could be deployed in quantities of tens of thousands if not more. Jamming attack on wireless networks was traditionally treated from the perspective of individual jammers. They advocate an approach based on the networked perspective, and using this networked approach and show that some interesting results can be obtained. In the paper, first, they demonstrated that DJN can cause a phase transition in the performance of the target network. They employ percolation theory to explain such phase transition, to analyze the impact of DJN on the connectivity of the target network, and to provide lower and upper bounds for the percolation of the target network to occur in the presence of DJN. Second, the author provides the scaling analysis of the jamming performance in relation to the jammer node density with the power density constraint. Third, they presented simulation results describing the impact of DJN topology on the jamming effectiveness.

## III. PROPOSED WORK

The proposed work will be the comparison of the effect of with and without Jamming attack in proposed routing protocol. The main concern is to maintain a counter of the number of requests served by various nodes. On the basis of number of requests in a particular time interval the decision will made whether to serve the node's request or not. The proposed work is implemented for the proposed routing protocol IAODV (Improved ad hoc on demand distance vector). In the proposed work, Jamming attack is implemented in IAODV and finally comparison will be made for with and without attack on the basis of various problems formed after the implementation of Jamming attack namely Constant Jammer, Reactive Jammer, and Random Jammer etc. Moreover, the comparison will be done on the basis of requisite parameters like Throughput and Packet Delivery Ratio

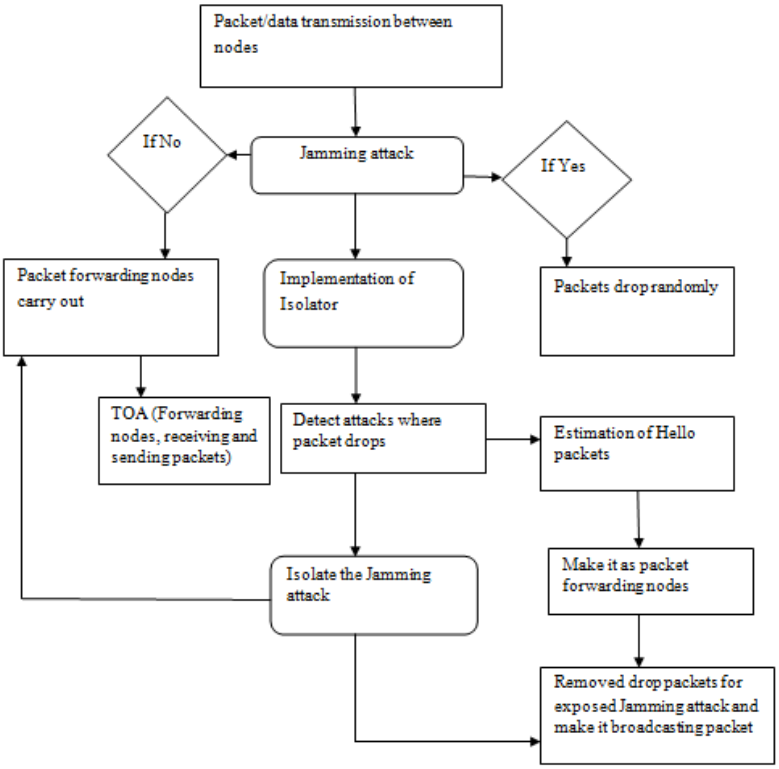


Fig.1 Algorithm structure for the proposed work

 

**Algorithm**

- Node I broadcast the neighbor discovery packet and collect neighbor node's echo message.
- Introduce the requisite functions and arguments and attach it to sequence number, labels and IAODV proposed routing protocol.
- Result analysis to distinguish the effect of jamming attack.
- Implement isolator to prevent the jamming attack.
- Result analysis and comparison for the desired parameters like throughput, pdr etc.

## IV. SIMULATION AND PERFORMANCE ANALYSIS

We use NS-2.35 simulation to carry out simulation. Since, NS-2 is an event-driven tool useful in studying the dynamic nature of computer network. It mainly provides the simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP)

| Parameter | Values |
|---|---|
| Simulator | NS-2 |
| Simulation Duration | 90 sec |
| Topology | 2500 meter X 2500 meter |
| No. Of nodes | 50 |
| Traffic type | FTP (TCP) |
| Routing protocol | IAODV |
| Channel Type | Wireless Channel |
| Mobility Model | Two Ray Ground Propagation Model |
| Network Interface Type | Wireless Phy IEEE 802.11 |

**Parameters Used for Comparison**

*Throughput*: is the average rate of successful message or packet delivered over a communication channel. The throughput is measured in kilo bits per second (kbps or Kbit/s). Greater the value of throughput means better the performance of the protocol.

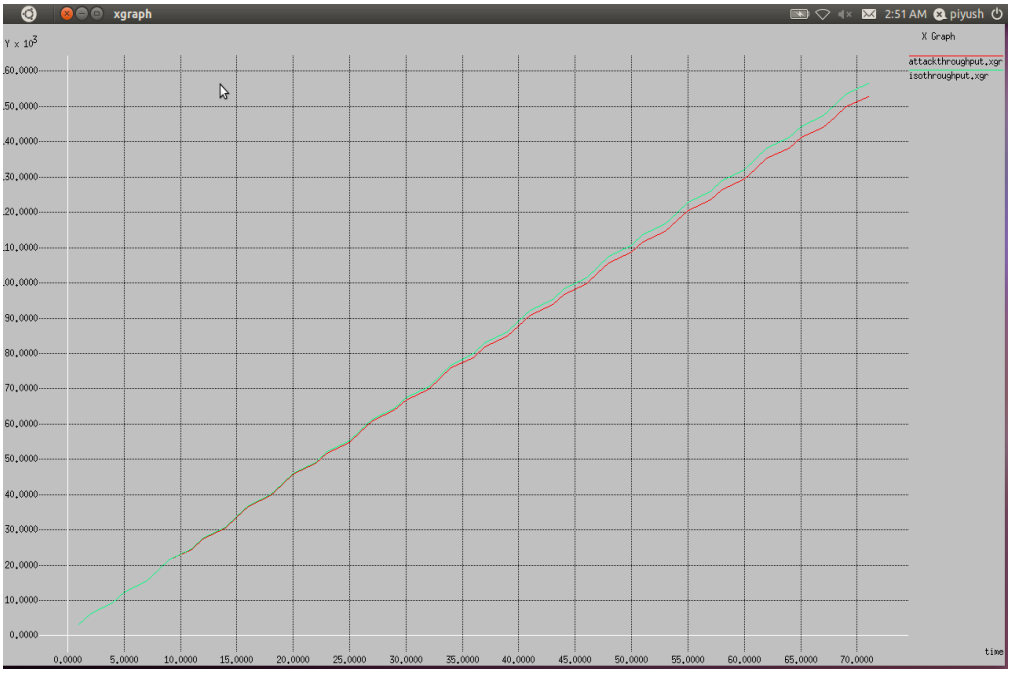


Fig.2: Throughput Comparison for with and without attack

The above Fig.2 clearly depicts the comparison graph of throughput for with and without attack. The green line for isolate (without attack) throughput is quiet better as compare to red line for proposed Jamming attack.

*Packet Delivery Ratio*: It is the ratio of the total packets delivered to the total number of sent packets.

 

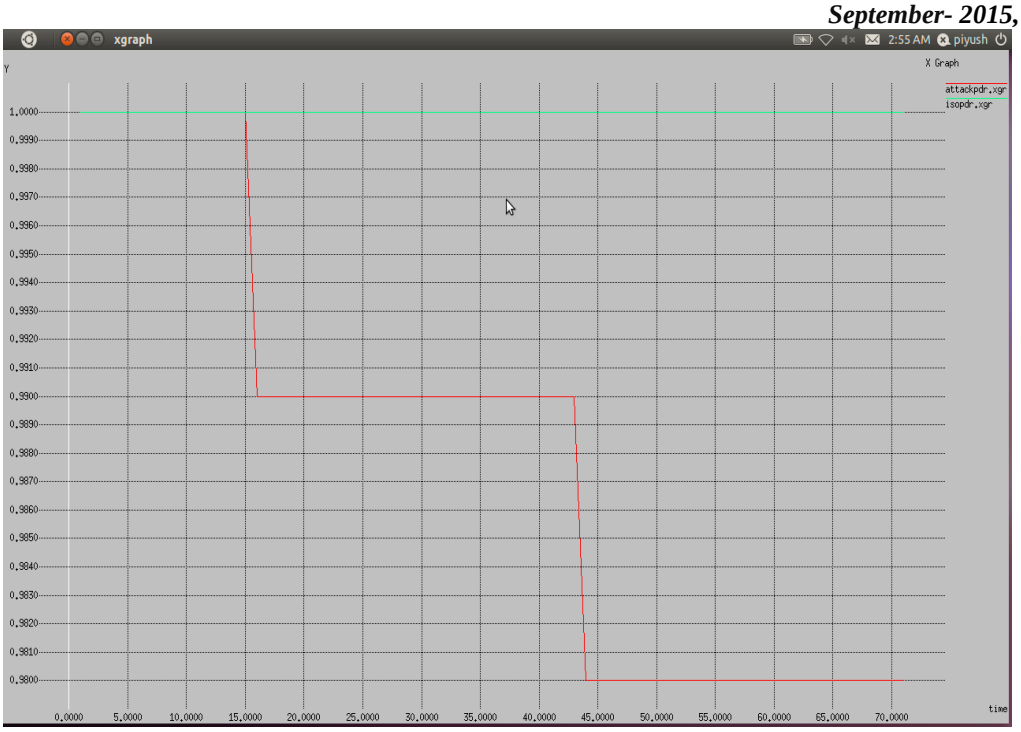


Fig.3 Packet Delivery Ratio Comparison for with and without attack

From the above Fig.3 clearly depicts that the PDR for without attack is constant and smooth as compare to with attack which is indicated by red line and represented as a downstairs.

## V. CONCLUSION AND FUTURE SCOPE

Nowadays, Security is a critical issue in the field of computer networks. They are more vulnerable to attacks and we have improved the quality and issues in Mobile Ad-hoc network and routing protocols. As jamming is a very serious threat to the normal operation of wireless networks, recently much research has been done to deal with it. All techniques are good from their point of view but not best from all points. The proposed work mainly deals with the effect of with and without jamming attack for the proposed routing protocol IAODV and found that the results of without attack (isolate.) is quiet better and optimist as compare to with jamming attack. The proposed work mainly deals in two parameters for comparison namely Throughput and PDR and the results clearly depict their performance evaluation.

Moreover, there is also need to work over some more metrics in future and also need to compare and evaluate their results for different attacks type which will be quiet helpful for security purpose in real life.

## REFERENCES

[1] Anthony D. Wood and John A. Stankovic(2004), “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks”, IEEE.

[2] Ashish Kumar Jain, VrindaTokekar(2011), “Classification of Denial of Service Attacks in Mobile Ad Hoc Networks”, IEEE, pp.no-256-261.

[3] Dressler, F. (2008),"A Study of Self-Organization Mechanisms in Ad Hoc and Sensor Networks” Elsevier Computer Communications, vol. 31 (13), pp. 3018-3029.

[4] GeethapriyaThamilarasu ,Sumita Mishra and Ramalingam Sridhar(2011), "Improving Reliability of Jamming Attack Detectionin Ad hoc Networks", IJCNIS, vol.3, no.1.

[5] Hong Huang, Nihal Ahmed, and PappuKarthik(2011), “On a New Type of Denial of Service Attack in Wireless Networks:The Distributed Jammer Network”, IEEE, , VOL. 10, NO. 7.

[6] ManasiSarkar, Debdutta Barman Roy(2011), “Prevention of Sleep Deprivation Attacks using clustering”, IEEE, pp.no- 391-394.

[7] Mohammed BOUHORMA, H. BENTAOUIT, A.BOUDHIR(2009), “Performance Comparison of Ad-hoc Routing Protocols AODV and DSR”, IEEE.

[8] KwangsungJu and KwangsueChung(2012), "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks", IJSIA, vol. 6, no. 2.

[9] Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague(2012), "All Your Jammers Belong To Us - Localization ofWireless Sensors Under Jamming Attack", IEEE.

[10] Selvamani K, Anbuchelian S, Kanimozhi S, Elakkiya R, Kannan A(2012), “A Hybrid Framework of Intrusion Detection System for Resource Consumption Based Attacks in Wireless Ad-Hoc Networks”, IEEE.

 

[11] Marco Tiloca, Domenico De Guglielmo, GianlucaDini and Giuseppe Anastasi(2013), "SAD-SJ: a Self-Adaptive Decentralized solution againstSelective Jamming attack in Wireless Sensor Networks", IEEE

[12] Longquan Li, Sencun Zhu, Don Torrieri*y*, SushilJajodia(2014), "Self-Healing Wireless Networks under InsiderJamming Attacks", IEEE

[13] G.Mahalakshmi, Dr.P.Subathra(2014), "A Survey on Prevention Approaches for Denial of Sleep Attacks in Wireless Networks", JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, vol-6, no1.

[14] Kasturiniva Das, Amar Taggu(2014 ),"A Comprehensive Analysis of DoS Attacks in Mobile Adhoc Networks", IEEE, pp. no- 2273-2278.

 