INFLUENCE WITH TRAFFIC RATE AND BEACON TIME FOR JAMMING ATTACK ON 802.11B IN MOBILE AD HOC NETWORKS

Jammana Lalu Prasad,
Department of Computer Science & Engineering,
Centurion University, Vizianagaram, AP, INDIA

Kavitha Chekuri
Department of Computer Science & Engineering,
Raghu Engineering College (A), Vishakapatnam, AP, INDIA

Lakshmana Rao Rowthu
Department of Computer Science & Engineering
Centurion University, Vizianagaram, AP.

Abstract— MANETs have distinctive characteristics like dynamic topology, wireless radio medium, restricted resources and lack of centralized administration; as a result, they're liable to differing types of attacks in several layers of protocol stack. Every node in a Manet is capable of acting as a router. The need for a secure Manet networks is powerfully tied to the protection and privacy options. This Jamming attacks are one in every of them. These occur by transmittal continuous radio ways in which to inhibit the transmission among sender and receiver. These attacks have an effect on the network by decreasing the network performance with buffer size, beacon amount varied as certained result on mobile ad-hoc network degrade the performance with Jamming attack. This work includes a network with high Mobility IEEE 802.11b with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP with high rate is being generated within the network. For the Simulation purpose we tend to utilized OPNET (Optimized Network Engineering Tool) MODELER 14.5 is employed for simulation. The performance of network is measured with relation to the QoS parameters.

Keywords— MANET, SANET, AODV, JAMMING, OPNET, OLSR, MODELER, WLAN, Route Discovery Time, Packet Drop.

I. INTRODUCTION
Ad-Hoc networks don't have any infrastructure wherever the nodes are liberal to be part of and left the network. The nodes are connected with one another through a wireless link. A node will function a router to forward the info to they don't have any centralized administration. Ad-Hoc networks have the capabilities to handle any haywire within the nodes or any changes that its expertise because of topology changes. Whenever a node within the network is down or leaves the network that causes the link between alternative nodes is broken. The affected nodes within the network merely request for brand spanking new routes and new links are established Ad-Hoc network are often categorized in to static Ad-Hoc network (SANET) and Mobile Ad-Hoc network (MANET).

JAMMING ATTACK
Jamming attack deliberately transmits of radio signals to disrupt the full communications by decreasing the signal-to-noise quantitative relation. The term Jamming is employed to

Figure1. Mobile Ad hoc Network

In our analysis work we have a tendency to be up the performance of mobile unintentional networks underneath Jamming attack by mistreatment associate degree integrated approach. The planned work includes a network with high Mobility, using IEEE along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high rate are being generated within the network.
differentiate it from unintentional jamming that known as interference. In Manet jamming may be a serious threat to its security. Jammers perpetually send.

II. LITERATURE REVIEW
Sisi Liu et al. (2012) addresses the matter of mitigating DoS attacks manifested within the sort of jam. The author thought of a complicated antagonist World Health Organization has data of the protocol specifics and of the science quantities won’t to secure network operations. This kind of antagonist can’t be prevented by opposing jam techniques that bank unfold spectrum. The author projected a brand new security metrics to quantify the flexibility of the antagonist to deny access to the management channel, and introduced a randomized distributed theme that enables nodes to ascertain and maintain the management channel within the presence of the transmitter. The projected technique is applicable to networks with static or dynamically allotted spectrum. Moreover, 2 algorithms for distinctive identification of the set of compromised nodes were projected, one for severally acting nodes and one for colluding nodes[19]. Dorus.R et al. (2013) proposes a mechanism for preventing jam attacks on wireless networks, examine the detection potency of jam attack and communication overhead of the wireless network exploitation proactive and reactive protocols. RSA formula is employed and analyzed for providing knowledge packets integrity data throughout wireless transmission. Through simulation and performance analysis, the enforced bar mechanism and also the integrity preservation provides higher packet delivery magnitude relation in proactive routing protocol (OLSR) than reactive routing protocol (AODV). Nadeem Sufyan et al. (2013) investigate a multi-modal theme that models totally different jam attacks by discovering the correlation between 3 parameters: packet delivery magnitude relation, signal strength variation, and pulse dimension of the received signal.

III. METHODOLOGY
A. Simulation Tool used:
This section describes the simulation tool used along with the proposed method. OPNET modeller v14.5 is extensive and a very powerful simulation tool with wide variety of possibilities. The entire heterogeneous networks with various routing protocols can be simulated using OPNET. High level of user interface is use in OPNET which is constructed from C and C++ source code blocks.

B. Simulation Setup:
The simulation work focuses on analyzing the performance of Manet below with and without jamming attack. So AN Integrated approach is employed to investigate the network performance below jam attack. This approach includes:

- High rate of 54mbps by victimisation IEEE 802.11b normal.
- Network with high quality
- Improved parameter of AODV routing protocol.
- Generation of high resolution FTP traffic.

C. Buffer management Methodology:
As long because the requests hit terribly slow rate the nodes might service the requests. Since the arrivals are freelance of every alternative, all the nodes might request for the service at an equivalent time, a condition of congestion might develop and node might not be ready to service all request. To beat this case it’s urged to use buffer to keep up a queue for such unfinished requests and to avoid packet drops.
Retransmission: Represents the full variety of bits (in bits/sec) forwarded from wireless local area network layers to higher layers altogether Wi-Fi nodes of the network. Retransmission is high for with transmitters once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 6.

Throughput (bits/sec): Represents the entire variety of bits (in bits/sec) forwarded from wireless local area network layers to higher layers all told WLAN nodes of the network. Throughput is high for with transmitters once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 7.

Delay (sec): Represents the full range of bits (in bits/sec) forwarded from wireless local area network layers to higher layers altogether wireless fidelity nodes of the network. Delay is high for with senders once compare with while not jammer for changed Beacon amount. Default Beacon amount is nice in Medium network as seen in Figure 8.
Route Discovery Time (sec): Represents the overall variety of bits (in bits/sec) forwarded from wireless LAN layers to higher layers altogether Wi-Fi nodes of the network. Route Discovery Time is high for with senders once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 9.

Total route error send: Represents the whole variety of bits (in bits/sec) forwarded from wireless local area network layers to higher layers all told WLAN nodes of the network. Total route error send is high for with senders once compare with while not jammer for changed Beacon amount. Default Beacon amount is nice in Medium network as seen in Figure 11.

Packet Drop: Represents the entire variety of bits (in bits/sec) forwarded from wireless computer network layers to higher layers altogether Wi-Fi nodes of the network. Packet Drop is high for with transmitters once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 10.
IV. CONCLUSION
Because of the wireless nature of mobile ad-hoc networks, numerous attacks are performed degrade the network performance. Jamming attack is one in every of them thus routing protocols are accustomed increase the network turn out. During this analysis work, Impact of jam Attack in Performance of Mobile improvement Networks. Jammers attacks can have an impression on network’s performance as a result of the jammers operates with the normal operation of the network. The result of attackers studied during this paper was by increasing delay, knowledge born traffic received and sent and decreasing packet drop qualitative relation of the network. During this analysis work, the network performance beneath jam attack is analyzing by applying integrated approach. This approach includes a network with high quality, IEEE 802.11g customary with Georgia home boy rate; serious traffic like FTP improved AODV parameters and inflated buffer size. In our paper, it absolutely was shown that jam attack reduces the network turnout, retransmission tries and will increase the media access delay.

V. REFERENCE