Efficient Detection and Prevention of Jamming Attack in MANET

Ashwinder Kaur
Department of Computer Science, Rimt-IET College, Gobindgarh

Abhilash Sharma
Assistant Professor
Department of Computer Science,
Rimt-IET College,
Gobindgar

ABSTRACT
Jamming attack is main problem and this can affect the network by various ways. Sometimes jammer retransmits messages to create jam over network or sometimes jammers are radio jammer which disturbs communication by decreasing the signal to noise ratio. In previous researches various techniques are discussed to detect jamming. One way is to check the signal busy ratio. If channel is busy for long time that means there is a jam on network or it can be check by checking the threshold value. If threshold value exceeds up to some limit then there expect some jam on network. When the jam will detected then check will be performed on the node which will be creating jam. Node identity will be checked by calculating the distance and the message of that node will be checked to detect the retransmission and replays. If sequence number will same than attacker will be detected but if sequence number is different message content will be checked. To check the reason of retransmissions an additional message will be send to destination so that if re-transmissions are due to the network failure it can be detected.

Keywords
WSN, Jamming attack.

1. INTRODUCTION

1.1 Mobile Ad Hoc Network (MANET)
MANETs stand for Mobile Ad hoc Networks. Mobile implies "mobility". Ad hoc is a Latin word and it means "for this only". MANET is an autonomous collection of mobile routers or nodes that communicate over wireless links. MANET is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its routable network properties where each node act as a "router" to forward the traffic to other specified node in the network.

1.2 Security Attacks
Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions.

These attacks can be classified into two types:

- **Passive Attacks:** Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it.
- **Active Attacks**: Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks can be internal or external.

1.2.1 Active Attacks

- **Black hole Attack**: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming.
- **Wormhole Attack**: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point.
- **Byzantine attack**: A compromised with set of intermediate, or intermediate nodes that working alone within network carry out attacks such as creating routing loops, forwarding packets through non -optimal paths or selectively dropping packets.
- **Flooding Malicious:** nodes may also inject false packets into the network, or create ghost packets which loop around due to false routing information, effectively using up the bandwidth and processing resources along the way.
- **Sinkhole**: In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So practically, the node eavesdrops on all the data.
- **Spoofing Attack**: in spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network.
- **Jamming**: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender.
- **Sybil attack**: The Sybil attack especially aims at distributed system environments. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods.
- **Denial of service attack** Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.

1.2.2 Passive Attacks

- **Traffic Monitoring**: It can be developed to identify the communication parties and functionality which could provide information to launch further attacks .It is not specific to MANET.
- **Traffic Analysis**: Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

2. RELATED WORK

Ismail, Z. et al[1] "Impacts of Packet Size on AODV Routing Protocol Implementation in Homogeneous and Heterogeneous MANET" Networks are being utilized as a part of different territories and the interest of clients these days has persuaded the development of the Mobile Ad Hoc Network (MANET). MANET is an element system without settled framework because of their remote nature and can be sent as multi-jump bundle systems. It is a remote system and has dynamic topology because of its hub versatility. There are two sorts of MANET, homogeneous and heterogeneous MANET. A structural planning has been planned in past work to model these two sorts of MANET. Three situations have been characterized from this structural engineering: situation I (correspondence totally inside MANET, homogeneous MANET), situation II (correspondence between MANET and remote LAN, heterogeneous MANET) and situation III (correspondence between MANET with remote LAN and wired LAN, heterogeneous MANET).

Thorat, S.A. et al [2] "Outline issues in trust based directing for MANET" In MANET hubs help one another in information steering. MANET functions admirably if the partaking hubs coordinate with one another. It is unrealistic to expect that, all hubs taking an interest in an open MANET are helpful and legitimate. For individual hubs it might be beneficial to be non-helpful and selfish. However non-participation, selfishness and malignant conduct of the taking part hubs may come about into breakdown of a MANET. Trust based directing calculations expect to distinguish making trouble and non-collaborating hubs in the MANET.

Durai, K.N. et al [3] "Vitality proficient irregular cast DSR convention with intervention gadget in MANET" Mobile Ad hoc systems (MANET) essentially have dynamic topology, as the directing framework's rundown of neighboring hubs and switches changes its area every once in a while. MANET's regularly expends parcel of transmission capacity, as the medium is imparted to different hubs. MANET hubs devours more power, regardless of the possibility that they don't participate in dynamic correspondence. The downside is fundamentally due to limits of the innovation and directing conventions accessible. MANET's are helpless against assault as they impart a remote medium to framework less spine.

Sheik, R. et al [4] "Security issues in MANET: A survey" Sometimes the physically dispersed registering gadgets in a system may be keen on figuring some capacity of their private inputs without revealing these inputs to each other. This sort of reckoning falls under the class of Secure Multiparty Computation (SMC). The answer for SMC issues in Mobile Ad hoc Networks (MANET) can be found with the adjustment of the information inputs or with some anonymization procedure. MANETs are the remote systems of the versatile registering gadgets with no backing of any altered base. The versatile hubs utilize any of the radio innovation like Bluetooth, IEEE 802.11 or Hiperlan for specifically corresponding with one another. The hubs carry on as hosts and in addition switches.

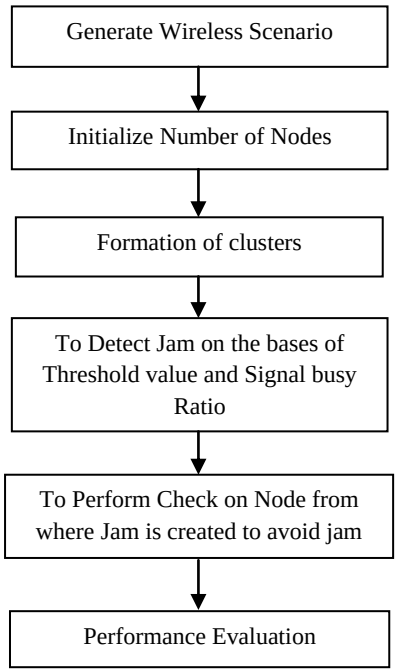
Rahman, F.M. et al [5] "4-N shrewd MANET directing calculation" Mobile Ad hoc Networks (MANET) utilize a correspondence method that can transmit information between hubs without the backing of settled base. MANET is a multi-bounce, self designing and self-governing system that can utilize transitional portable hubs as a switch and transmit information between cell phones. A quadrant based clever vitality controlled multicast calculation for MANET distinguished amid prior examination is the premise for the calculation exhibited in this paper. Recreation results and correlation with other MANET directing calculations highlighted that the calculation is vitality productive and solid yet generally abate for information transmission.

3. PROBLEM FORMULATION

In wireless networks jamming attack is main problem and this can affect the network by various ways. Sometimes jammer retransmits messages to create jam over network or sometimes jammers are radio jammer which disturbs communication by decreasing the signal to noise ratio. Jamming can also be arise because of various different reasons like it can be intentionally created by attackers which lead to denial of service attack or it can be unintentionally created on network due to congestion. In previous researches various techniques are discussed to detect jamming. One way is to check the signal busy ratio. If channel is busy for long time that means there is a jam on network or it can be check by checking the threshold value. If threshold value exceeds up to some limit then there expect some jam on network. But there is still some work can be done. This attack can be prevented by blacklisting the nodes. It can be possible by applying check on nodes.

- To set threshold value to detect the jam over network.
- To check signal busy ratio to detect jam.
- To check identity of node.
- To calculate distance on the bases of which identity will be check.
- To evaluate some of the QOS parameters.

4. PROPOSED WORK



First of all we generate the wireless scenario. Then Initialize the number of nodes. Cluster formation will be achieved and then jam will be detected on the bases of threshold and signal busy ratio. When the jam will detected then check will be performed on the node which will be creating jam. Node identity will be checked by calculating the distance and the message of that node will be checked to detect the retransmission and replays. If sequence number will same than attacker will be detected but if sequence number is different message content will be checked. To check the reason of retransmissions an additional message will be send to destination so that if re-transmissions is due to the network failure it can be detected.

Simulation Table

Channel Type	Wireless
Propagation	Two way-ground
Mac Type	802.11
Queue Type	Drop tail
Antenna Type	Omni
Topography Dimensions	1900*1200
Number of nodes	50
Simulation Time	22 sec
Range	200-500 m

5. RESULTS AND DISCUSSIONS

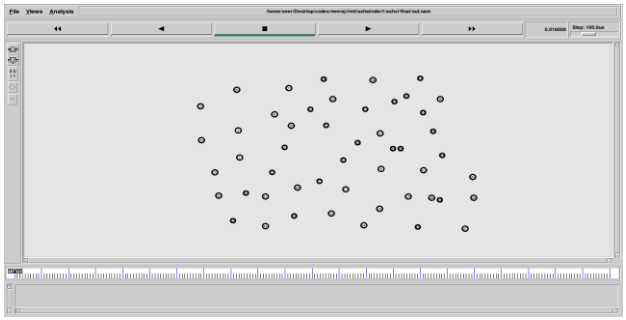


Fig 5.1: Initialization of nodes

This Scenario is use to represent the initialization of nodes

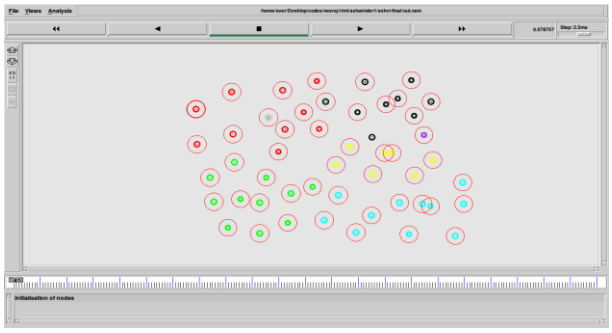


Fig 5.2: Routing between nodes

This Scenario is use to represent the routing take place between the nodes. Due to routing the data transmission take place between the nodes.

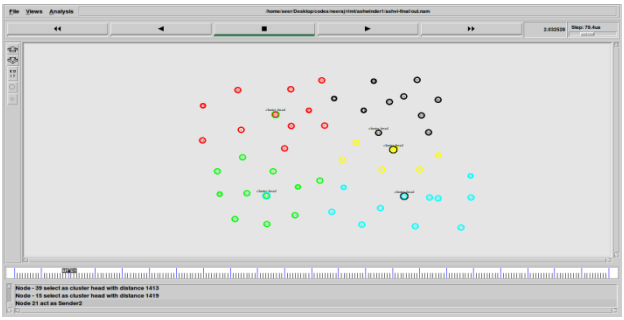


Fig 5.3: Selection of Cluster Head

This figure is use to represent the selection of cluster heads. In this scenario we have 5 cluster head.

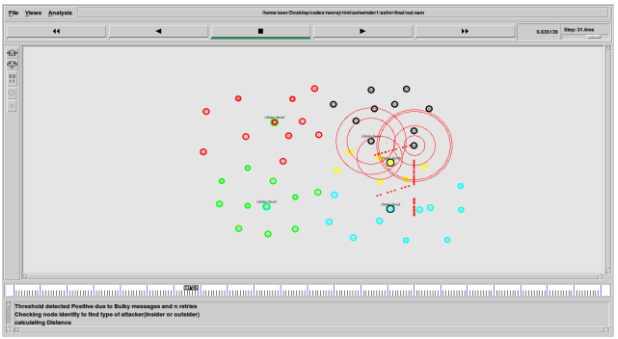


Fig 5.4: Jamming Attack occurred in nodes

This scenario is use to represent the jamming attack occur between the nodes. Jamming attack deliberately transmits of radio signals to disrupt the whole communications by decreasing the signal-to-noise ratio. The term jamming is used to differentiate it from unintentional jamming which called interference. In MANET Jamming is a serious threat to its security. Jammers constantly send repeated signals (in affected area) to interfere with the communication between nodes in the network.

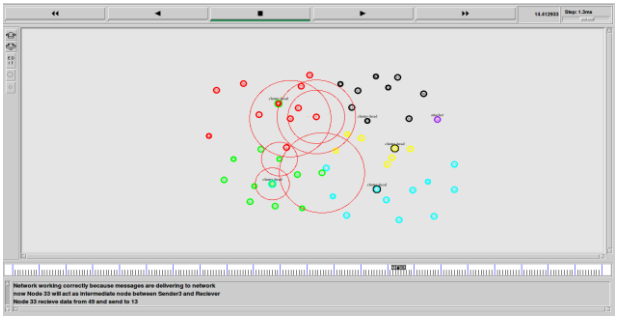


Fig 5.5: Black list

This scenario is use to represent the black listed nodes.

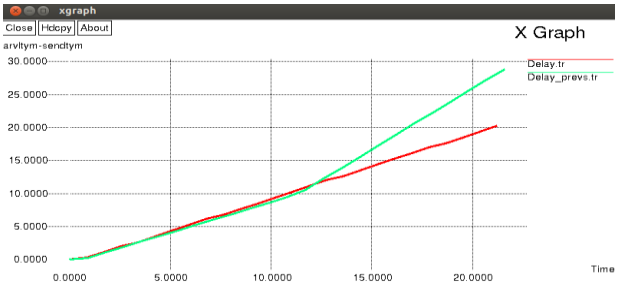


Fig 5.6: Packet Delay

This includes all possible delays caused by buffering during route discovery, latency, and retransmission by intermediate nodes, processing delay and propagation delay. It is calculated as

$$D = (T_r - T_s)$$

Where, T_r is receive time and T_s is sent time of the packet.

Table 5.1: Delay

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
5	2.77	2.64
10	6.94	6.76
15	12.22	11.17
20	20.55	15.29
25	28.88	20.29

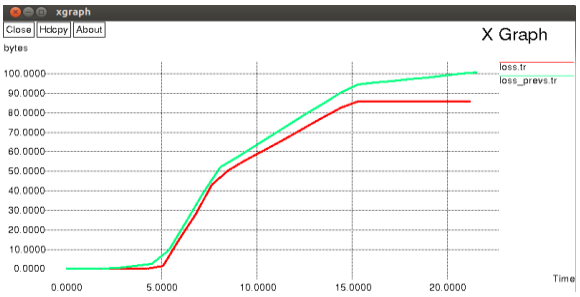


Fig 5.7: Packet Loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. The Transmission Control Protocol (TCP) detects packet loss and performs retransmissions to ensure reliable messaging. Packet loss in a TCP connection is also used to avoid congestion and reduces throughput of the connection.

Table 5.2: Delay

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
5	1.53	0.0
10	52.28	43.02
15	79.42	69.0
20	96.29	85.72
25	100.89	85.72

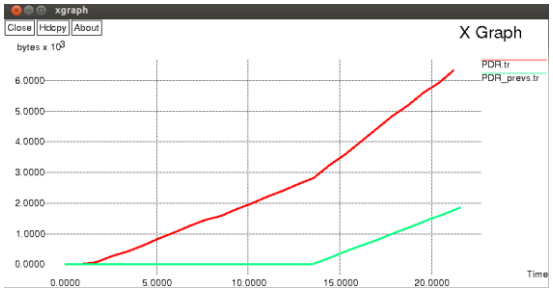


Fig 5.8: Packet Delivery Ratio

It is the ratio of all the received data packets at the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the no. of packet originated from the source.

$$PDR = (P_r / P_s) * 100$$

Where, P_r is total packet received and P_s is total packet sent.

Table 5.3: PDR

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
5	0.0	419
10	0.0	1454
15	0.0	2420
20	828	4007
25	1863	6353

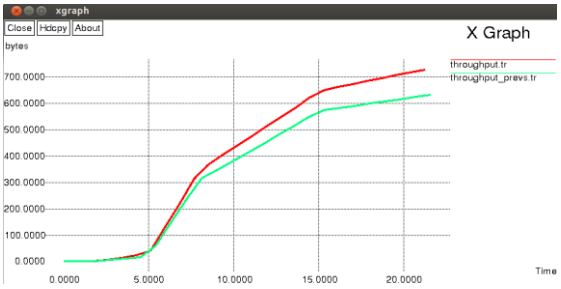


Fig 5.9: Packet Throughput

It is the average at which data packet is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.

Throughput = (no of delivered packets * packet size) / total duration of simulation

Table 5.4: Throughput

Time (in sec)	Previous Work	Present Work
0	0.0	0.0
5	16.69	13.78
10	315.77	314.85
15	478.71	511.73
20	511.85	662.82
25	632.55	729.17

6. CONCLUSION

MANETs stand for Mobile Ad hoc Networks. Mobile implies "mobility". Ad hoc is a Latin word and it means "for this only". Jammer retransmits messages to create jam over network or sometimes jammers are radio jammer which disturbs communication by decreasing the signal to noise ratio. Jamming can also be arise because of various different reasons like it can be intentionally created by attackers which lead to denial of service attack or it can be unintentionally created on network due to congestion. In previous researches various techniques are discussed to detect jamming. One way is to check the signal busy ratio. If channel is busy for long time that means there is a jam on network or it can be check by checking the threshold value. If threshold value exceeds up to some limit then there expect some jam on network. But there is still some work can be done. This attack can be prevented by blacklisting the nodes. We got various types of parameters we conclude that our system gives us better results.

7. REFERENCES

[1] Ismail, Z., Hassan, R. "Effects of Packet Size on AODV Routing Protocol Implementation in Homogeneous and Heterogeneous MANET" *Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM), 2011*, pp. 351 – 356

[2] Thorat, S.A., Kulkarni, P.J. "Design issues in trust based routing for MANET" *International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2014*,pp. 1 – 7.

[3] Durai, K.N., Baskaran, K. "Energy efficient random cast DSR protocol with mediation device in MANET" *International Conference on Advanced Computing and Communication Systems (ICACCS), 2013*, pp. 1 – 5.

[4] Sheikh, R., Singh Chande, M., Mishra, D.K. "Security issues in MANET: A review" *Seventh International Conference On Wireless And Optical Communications Networks (WOCN), 2010*, pp. 1 – 4

[5] Rahman, F.M., Gregory, M.A. "4-N intelligent MANET routing algorithm" *Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011*, pp. 1 – 6.

[6] Shah, N., Depei Qian "Cross-Layer Design to Merge Structured P2P Networks over MANET" *16th International Conference on Parallel and Distributed Systems (ICPADS), 2010*,pp. 851 – 856.

[7] Moradi, Z.,Teshnehlab, M., Rahmani, A.M. "Implementation of neural networks for intrusion detection in manet" *International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), 2011*, pp. 1102 – 1106.

[8] Capt. Dr. S. Santhosh Baboo and Mr. V J Chakravarthy, "An Improvement In Congestion Control Using Multipath Routing In MANET – Right Angled And Ant Search Protocol (RAAA)" *The International Journal of Computer Science & Applications (TIJCSA), Volume 2,2010*,pp. 45-49.

[9] Vicomsoft, "Knowledge share whitepapers wireless networking Q&A", Vicomsoft connect and protect, Jan 2003.

[10] Wikipedia, "The free encyclopedia-, Mobile ad-hocNetwork", http://en.wikipedia.org/wiki/Mobile_ad-hoc_ network, Oct-2004.

[11] Charles E.Perkins and Elizabeth M. Royer, "Ad hoc on demand distance vector (AODV) routing (Internet-Draft)", Aug-1998.

[12] Humayun Bakht, "Computing Unplugged, Wireless infrastructure, Some Applications of Mobile ad hoc networks", http://www.computingunplugged.com/issues / issue200410/00001395001.html, April-2003.