IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-3 E-ISSN: 2347-2693

A Novel Technique to Isolate and Detect Jamming Attack in MANET

Harkiranpreet Kaur[1*] and Rasneet Kaur[2]

[1*,2] *Dept .of CSE, I.K. Gujral Punjab technical University, India*

www.ijcseonline.org

Received: Feb/22/2016 Revised: Mar/01/2016 Accepted: Mar/14/2016 Published: Mar/31/ 2016

Abstract— MANET is infrastructure less, decentralized multi hope network where the nodes are randomly to move in any direction, there each node works as a router and host to send packet to each other, there is no any requirement of fixed infrastructure. There are many security threats in MANET. Various types of attacks can be easily triggered in the network. So MANET has a security issue. In this paper we have discussed about Jamming attack in AODV protocol. Due to this attack network performances degrade. Therefore a novel technique has been proposed to detect and isolate jamming attack in the network using monitoring nodes.

Keywords— MANET, Attacks, Grayhole, Throughput, ZRP, internal attacks

1. Introduction

MANET is a mobile ad-hoc network. An ad-hoc network is set of wireless mobile nodes that have ability to communicate with each other without the help any centralized administration [1]. MANET has a dynamic topology due to the mobility of nodes. Wireless network contain collection of mobile hosts (nodes) that are communicate with each other through the wireless links. MANET is infrastructure less, decentralized multi hope network where the nodes are randomly to move in any direction, there each node works as a router and host to send packet to each other, there is no any requirement of fixed infrastructure. MANET provide successful solution in several cases, where any wired or wireless infrastructure is not accessible damaged or destroyed and overloaded due to some reason such as military operations, emergency and rescue operations, disasters relief efforts and tactical batter field; as well as conferences and class rooms or in research area like a sensor network [2]. MANET is network which is fully distributed and able to work at anywhere without the help of any centralized administration or access points or base stations.

Fig.1.1 MANET Network

1.1 Challenges in MANET: There are many challenges in MANET which are as follows:

1.1.1 Routing: The most common challenging issue in MANET is Routing data packets in between nodes when there is change in the topology. Another challenge for MANET is multicast routing because the nodes are move randomly in the network. Several of the protocol based on the reactive routing rather than proactive routing [2].

1.1.2 Security and Reliability: In an ad-hoc network security is a biggest problem due to the nasty neighbors that are relaying on the information. So there we need of some security mechanism such as the authentication and the management of key to provide the security to each node in MANET. Another problem introduced in MANET is due to the wireless links that have finite transmission area is reliability[3].

1.1.3 Quality of service (QOS): The common challenge in changing environment is providing the different quality of service level. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services [1].

1.1.4 Inter-networking: To interact with an ad-hoc network, inter-networking between MANET and infrastructure network is often expected in many terms. The coexistence of routing protocol for mobile hosts is a challenge to manage the speed of nodes.

1.1.5 Power consumption: For various light-weight mobile devices, the communication related function should be optimized for lean power consumption. Conservation of power and power aware mobility management [4].

1.1.6 Multicast: Multicast is able to support multi-party wireless interaction. The multicast routing protocol must be able to deal with the speed of nodes that include any time leave or join the network, so the multicast tree is no longer static.

1.2 Attacks in MANET: The higher challenging issue in MANET securing wireless ad-hoc network to provide the better security solution first we require to know about the type of attacks to protect the information transmission from the attacks. There are various kinds of attacks available in the MANET. It is classified into two groups:

1.2.1 Active attack: There are two type of Active attacks are known as external as well as internal attacks. Active attacks are the attacks that disturb the network performance and task by sending the wrong or modified information and false message [5].

1.2.1.1 Internal attacks: Internal attacks are attackers that are present inside the network. In internal attacks the attacker nodes that belong to network take unauthorized access and deal as are normal node to disrupt the network. These nodes analyze the traffic between other nodes and also take part in other network activities.

1.2.1.2. External attacks: External attacks are attacker that not belongs to the network or outside the network. External attacks are attacks that done by the nodes that are outside the network or which is not present in the network. For example: jamming, modification and message reply.

1.2.2 Passive attacks: Passive attacks are attacks that are difficult to find on the network and does not disturb the network task, performance and operations. The example of passive attacks is traffic analysis and traffic monitoring [6].

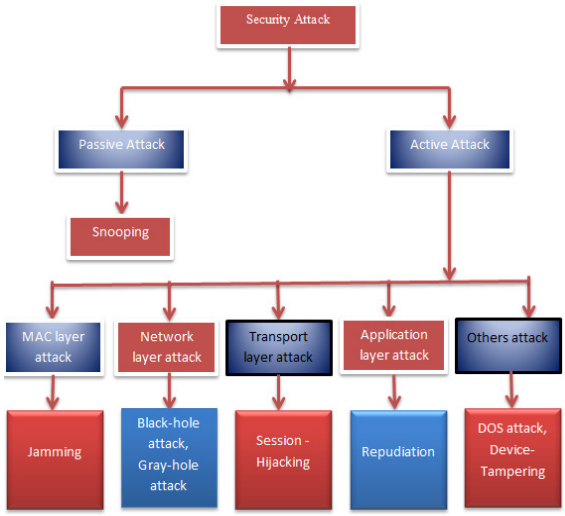


Fig.1.2 Security Attacks in MANET

2. Review of Literature

In this paper [3], simulation of secure AODV protocol is carried out by using various simulation parameters such as no. of mobile nodes, routing protocol, traffic, and transport protocol and packet size. Performance metrics PDR, end to end delay and packet delivery ratio are used to check the performance of network. Simulation is carried out by using NS2. In this paper the author provide the method to detect and prevent of gray-hole attack and also to know the behavior of malicious node. The algorithm is provides the better solution to improve the performance of ad-hoc. In this paper [4] they have compared AODV, DSDV, DSR and ZRP protocol using the tool NS2 and was compared in term of packet delivery ratio, average delay, routing overhead and average throughput. In order to evaluate the performance of the protocols network size was 1200m x 1200m. Antenna model was Omni directional, simulation time was 10 second and the traffic type was CBR (constant bit rate) and number of nodes varies. The author have concluded that, in case of packet delivery ratio, AODV has better performance when number of nodes increase, packet delivery ratio also increase, DSDV performance is worst in this case. Average throughput of AODV was better while the DSDV was worst performance. In case of routing overhead ZRP has better performance. Due to smaller zone radius and DSR was worst. In case of average delay ZRP was better performance due to minimum delay, ODV is worst because the higher drop. In this paper [5,8,9] author compared the routing protocols (DSDV, DSR, and ZRP). They have used the network simulator NS2 and were compared in term of packet delivery ratio and throughput by varying the pause time and the number of nodes. In simulation environment, they have constructed, the network area 500m x 500m, traffic type CBR (constant bit rate), antenna type was omni and packet interval 0.2 sec, radio propagation model was two ray ground. Number of nodes and pause time varying in this scenario. Simulation was carried out using NS2.33. They have concluded that DSR performance is same for different pause time while DSDV and ZRP when pause time increase packet delivery fraction decrees. When the number of nodes rises up, the packet delivery fraction decrease but still maximum in case of DSR as compare to DSDV and ZRP but ZRP have better performance in case of lesser number of nodes as compare to DSDV, ZRP performance goes down when no. of nodes increase. In case of throughput was increase when pause time increase for all DSDV, DSR and ZRP but maximum for DSR. But when pause time increase throughput DSDV and ZRP almost same. In term of no. of nodes increase the throughput of DSR increase but decrees for the ZRP when no. of nodes increases. In this paper they introduced [6,10,11] about the study threats faced by the ad hoc network environment and provide an arrangement of the various security mechanisms. The strengths and vulnerabilities of the existing routing protocols analyzed and suggest a broad and comprehensive framework that can provide a tangible solution. In this paper [7,12] author discussed various mutual authentication schemes of mobile ad hoc network. They had discussed the symmetric key and asymmetric key distribution schemes. They had also discussed PKI (public key distribution) scheme which based on the symmetric key distribution scheme. In this paper author proposed a new authentication scheme named as

MOCA which hybrid type of scheme and use both PKI and asymmetric schemes for mutual authentication.

3. Jamming Attack in MANET

A jammer is an entity whose main aim is to trying to get in the way with the physical transmission and reception of wireless communications. A jammer constantly emits RF signals to fill a wireless channel so that legal traffic will be completely blocked. The common characteristics for all the jamming attacks are that their interactions are not amenable with MAC protocols [2,13]. The ratio of packets that are effectively sent out by a justifiable traffic source compared to the number of packets it intends to send out at the MAC layer. In this attack number of source are formed instead of single source which sends rough packets to the transmission channels and jammed the channel. Due to this jamming, packet loss starts. This decrease the efficiency and reliability of the system. Due to this attack many problems are arise like channel becomes busy, delay in transmission, new packet drops begin due to buffer space full etc [5,14].

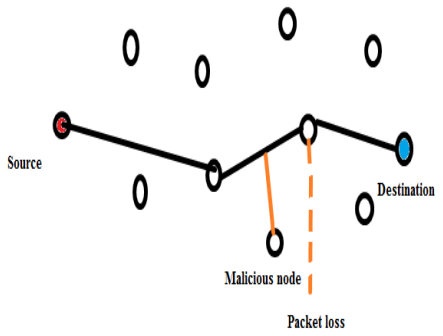


Fig.1.1 Jamming Attack

In above fig. 1.1, there are number of nodes in the network. Source sends packet and destination receive it according to DSR protocol. There is a malicious node in the network which injects fake packets on the path. Due to packet injection on the network, it jams and starts packet loss due to jamming at the network.

4. Proposed Methodology

The proposed methodology will detect the malicious node and isolate, it from the network. The methodology is based on the throughput of the network. When the throughput of the network, will degrades to certain threshold value, nodes in the network will go to monitor mode and detect the malicious node.

In our proposed work we overcome the problem of dropped packet by detecting them and redirect to the source with the help of monitoring nodes.Suppose we have a network in which number of nodes are present. There are two ways in which packets are transferred from source to destination. First of all source sends fake packets for the route establishment from source to destination. We can also say that source sends fake messages. Secondly source flood the packets in the network as data packets. The node which received data packets goes to the monitor node. In this process source generate ICMP packets that flood in the network. The nodes which receives them as a data packet goes to the premicous node or monitor node. After receiving monitoring packets other nodes than monitor nodes in the network, they start monitoring intermediate nodes from source to destination. Monitor node sends packets on route. It does not send data packets but send random packets in the network. Now the nodes which receive the packets forward it to the destination and consider that path as a route. But the monitor nodes also monitoring those nodes which drop the packet that is malicious node dropped the packets or send it to the destination through other paths. Monitoring nodes detect that node which further does not send it to the destination. So the nodes which detect the malicious node reply to a source node expect route node so that source isolate the path and stop forwarding more packets.

ALGORITHM

Start( )

1. Deploy the wireless ad hoc network with fixed number of mobile nodes and in fixed area
2. Select the shortest path between the source and destination using AODV routing protocol
3. The source node send fake messages to destination to verify the route

   To verify the route
   {
4. Source flood the monitor mode in the network
5. The nodes after receiving the monitor mode message start monitoring the route between source and destination
   If (Malicious node ==exits)
   {
   1. The other nodes in the network send malicious node information to source
   2. The source isolate the selected path
   3. The source select the other best path
6. Else
   {
   The source keeps on communicating with destination
   }

End

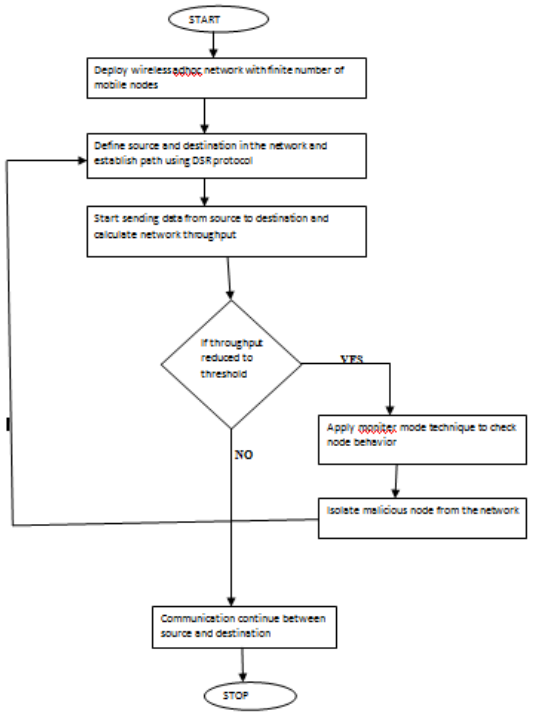


Fig 2: Flowchart of proposed technique

5. Experimental Results

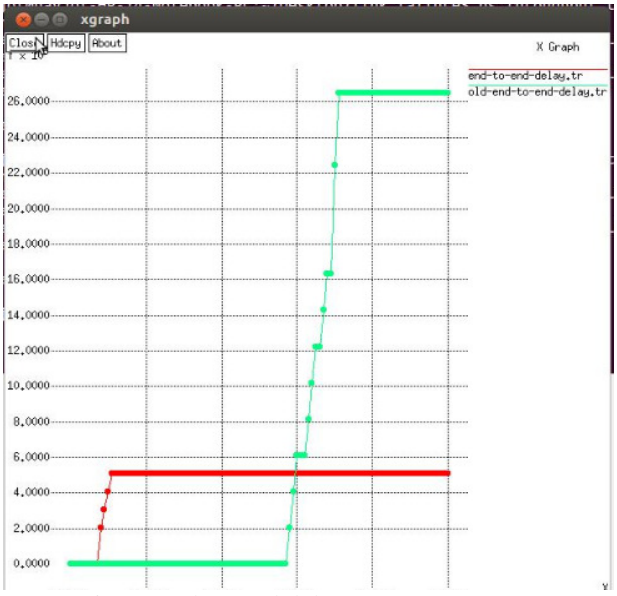
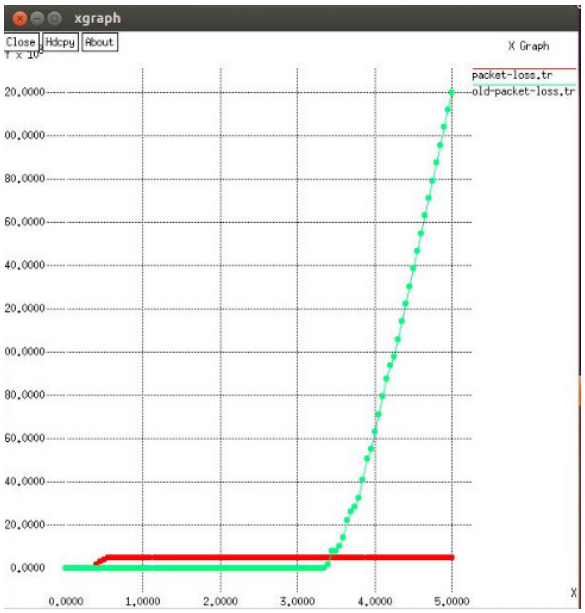


Fig. 1: End-to-End delay

In figure 1, end-to-end delay is represented. Red line shows old energy and green lines show end-to-end delay. New proposed system has less delay as compared to the existing system. So new technique is more efficient.



In this graph packet loss is less in new proposed than the existing system. Red lines shows less packet loss of new system and Green lines shows more packet loss in existing system.

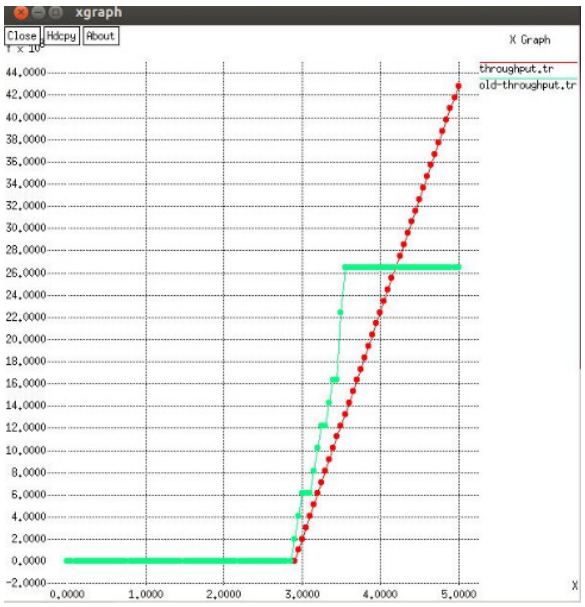


Fig.1.3Throughput

In fig.1.3 throughput is more in new proposed than the existing system. Red lines shows more throughput of new system and Green lines shows less throughput in existing system.

6. Conclusion

Now days, Security of the network is most important and very biggest challenge in Mobile Ad-Hoc Network. There

are various kind of security attacks are possible in the Ad-Hoc network. Jamming Attack is one of the most common security attacks on the network layer in MANET. Due to, malicious behavior to detect the jamming Attack is from network is difficult than the Black –Hole attack. In this attacker can attack on the compromise nodes to make them malicious node. There can also possibility of more than one malicious node in the network. In this attack malicious node drop the packets rather than forward these packets to make the performance of network inefficient.so there is need of the proper and perfect mechanism to detect and remove the jamming Attack from the network to improve the performance of network such as to increase the Packet delivery ratio and Throughput and decrease the End-to-End Delay. In this paper, a novel technique has been proposed to detect and isolate jamming attack to increase network performance.

References

[1] Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", *IEEE, 2009*

[2] Ashish K. Maurya, D. S. (Nov,2013). "Simulation based Performance Comparison of AODV, FSR and ZRP Routing Protocolin Manet". *IJCA* , 23-28.

[3] Awadesh Kumar, P. S. (July,2013). "Performance Anaysis Of AODV ,CBRP,DSDV and DSR MANET Routing Protocols using NS2 sIMULATION". *I.J Computer Network and Information Security* , 45-50.

[4] Meenakshi Jamgade and Vimal Shukla , "Comparative on AODV and DSR under Black Hole Attacks Detection Scheme Using Secure RSA Algorithms in MANET", International Journal of Computer Sciences and Engineering, Volume-04, Issue-02, Page No (145-150), Feb -2016.

[5] Divangna Gupta, R. K. (aug,2014). Simulationof Different Routing Protocols in MANET Using NS2. *International journal of Scientific and Research Publication* , 1-5.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,*Springer ,2006*

[7] Smita Das, "Routing table of DSDV in Mobile Ad-hoc Networking", International Journal of Computer Sciences and Engineering, Volume-03, Issue-10, Page No (48-51), Oct -2015, E-ISSN: 2347-2693.

[8] M Ravi Kumar, D. G. (2013). "Performance Evaluation of AODV and FSR Routing Protocol in MANET. *GJCST* , 1-7.

[9] Onkar V.Chandure, A. P. (NOV,2012). Simlation of secure AODVin Gray-hole Attack for Mobile ad-hoc Network. *IJAET* , 67-75.

[10] Onkar V.Chandure, P. (2011). "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV Routing protocol in MANET". *IJCSIT* , 2607-2611.

[11] Preeti Gharwar, M. S. (April,2013). "Performance Comparison Of Routing Protocols". *IJARCCE* , 1920-1924.

[12] Rutvij H. Jhaveri, D. C. (2012). "A Novel Gray Hole and Black Hole Attacks in Mobile Ad-Hoc Networks". *International Conference on Advanced Computing& Communicaion Technologies"* , 556-560.

[13] Virali Girdhar and Gaurav Banga, "A Comparative Analysis of Different Movement Models in MANET", International Journal of Computer Sciences and Engineering, Volume-03, Issue-06, Page No (9-13), Jun -2015

[14] S onam Gupta and Rekha Sharma," A QoS Based Simulation Approach of Zone Routing Protocol in Wireless Ad-hoc Networks ", International Journal of Computer Sciences and Engineering, Volume 2, issue 7, P.No 24-30, 2014

AUTHORS PROFILE

Harkiranpreet Kaur pursed Bachelor of technology from I. K. Gujral punjab technical university, India in 2013 and is pursuing master of technology from the same.

Rasneet Kaur has pursued her bachelor of technology and her master' of technology from Punjabi university Patiala. She is working as an assistant professor in shaheed udham singh college of engineering and technology from many years.