To Propose a Novel Technique for Link Recovery in MANET

Amanpreet Singh (Student), Bhupinder Kaur (Assistant Professor)

Abstract: As we know MANET is a self-configuring and infrastructure less wireless network. It can be move independently in any direction. There is no pre-existing infrastructure is available for the MANET. Malicious nodes are present easily which is vulnerable to attack. Security is the major challenge in wireless network. The security should be strong so that information can be transfer without any misbehavior. There are number of attacks possible in wireless sensor network to encrypt the data. So to avoid this mutual authentication between all the nodes should be necessary. Therefore link failure problem occurs during data transfer. In this paper, a novel technique has been proposed to overcome link failure problem based on energy.

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.

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 provides the better solution to improve the performance of ad-hoc performance. In this paper [4], they discussed many challenges and issues. An ad hoc network is a collection of mobile nodes that dynamically form a temporary network, without the use of existing infrastructure. When two nodes are not within the radio range of one another, they use intermediate nodes to route packets for them. Routing in MANET is a challenging problem which draws researcher's vision, due to nodes mobility, dynamic topology, frequent link breakage, limitation of nodes (memory, battery, bandwidth, and processing power), and lack of central point like base stations or servers. So by analyzing and comparing different ad hoc routing protocols based on the metric throughput, packet delivery ratio, end to end delay which may give a solution to the challenges in the ad hoc routing in different situations. The mobility of nodes and instability of the wireless environment may result in link breaks between neighboring nodes, even causes the route to be invalid. This paper focuses on the mobility of the source node and intermediate node which may result link failure. If a source node moves, it is able to reinitiate the Route Discovery. In this paper [5] author compared the routing protocols. 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. In this paper [6], they discussed about AODV and most of the on demand ad hoc routing protocols use single route reply along reverse path. Rapid change of topology causes that the route reply could not arrive to the source node, i.e. after a source node sends several route request messages; the node obtains a reply message, especially on high speed mobility. This increases both in communication delay and power consumption as well as decrease in packet delivery ratio. To avoid these problems, a "Backward AODV (B-AODV)" which tries multiple route replies. Backward AODV (B-AODV), which has a novel aspect compared to other on-demand routing protocols on Ad-hoc Networks: it reduces path fail correction messages and obtains better performance than the AODV and other protocols have proposed. Backward AODV provides good results on packet delivery ratio, power consumption and communication delay. Successful delivery of RREP messages are important in on-demand routing protocols for ad hoc networks. The loss of RREPs causes serious impairment on the routing performance. This is because the cost of a RREP is very high. If the RREP is lost, a large amount of route discovery effort will be wasted. Furthermore, the source node has to initiate another round of route discovery to establish a route to the destination. They proposed the idea of "BACKWARD AODV (B-AODV)", which attempts backward RREQ. B-AODV route discovery succeeds in fewer tries than AODV. They conducted extensive comparison study to evaluate the performance of B-AODV and compared it with AODV. B-AODV improves the performance of AODV in most metrics, as the packet delivery ratio, end to end delay, and energy consumption.

3. Link Failure in AODV

Link failure is a main problem in AODV which is responsible for the performance degradation and packet lost. Suppose we have number of nodes in our network. Source is host node from where data has to be send and destination node is final node. Any active node which is responsible for the updating of table entry. When source node move, new route discovery initiated. If intermediate nodes or the destination move then following conditions possible:

1. he next hop links break resulting in link failures.
2. Routing tables are updated when link failure occurs.

3. All active neighbors are informed by Route Error message.

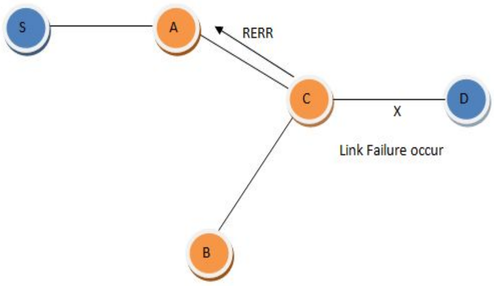

Fig.3.1 Link Failure

In the above Fig. 3.1, link between C and D breaks. Now node C invalidate route D in the route table. Node C creates Route Error message and lists all destinations that are now unreachable and sends to upstream neighbor this messages.

4. Proposed Methodology

This work will have the broader scope. Enhancement in AODV is required so that to overcome the problem of link failure during data transfer from host to destination. First of all mutual authentication is required between the mobile nodes to prevent the various inside and outside attacks. When the mobile nodes are mutually authenticated, it leads to the reliable data transmission between the mobile nodes. But the main problem occurs during the failure of the link. Due to link failure packet is lost easily. In proposed work, enhancement in AODV concept is important. This protocol is designed to provide best path according to signal strength. The path which has maximum energy will choose as a final path. This work will helps to reduce the problem occur in link failure and packet lost problem. Now the performance degradation problem will also improve.

5. Experimental Results

The whole scenario has been implemented in NS2.

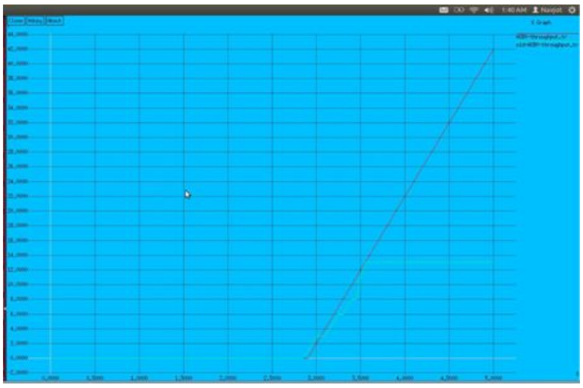

Fig.5.1 Throughput

In throughput graph the figure illustrated the throughput of the new and previous technique. The green line shows the throughput of the network in previous technique. The throughput of the new technique is shown in red line. The efficiency of the enhanced AODV increase with the help of energy. The throughput the network is enhanced through the use of new proposed technique because the packet loss in the network is reduced. The results help to improve the performance of the system.

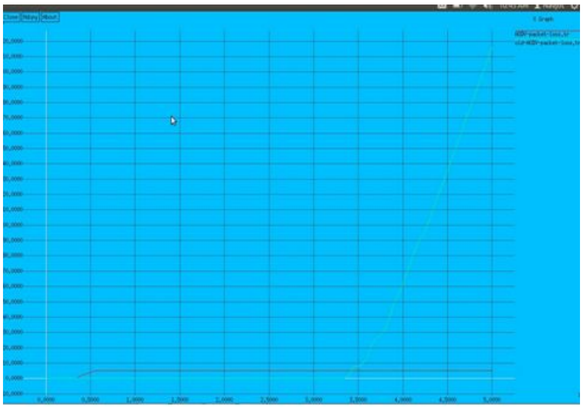

Fig.5.2 Packet Loss

During link failure problem packet loss occur in old AODV. But this problem can be overcome signal strength in enhanced AODV. Here x-axis represents time and y-axis represents no. of packets. Red line shows new AODV and green line old AODV. This shows that packet loss is less in new AODV as compared to old AODV.

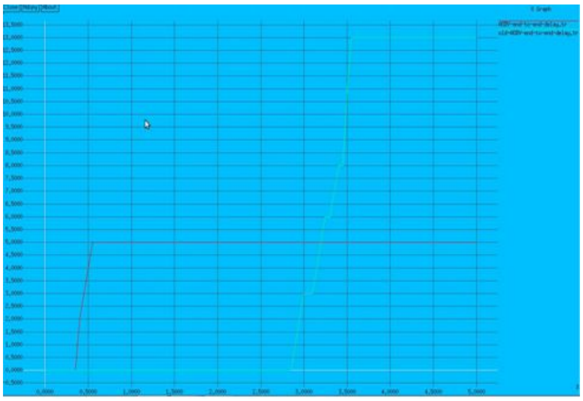

Fig.5.3 Delay

Delay graph represents that old AODV has more delay than new AODV. Thus transmission is fast in new AODV which helps to improve performance. Red line represents new AODV and green line represents old AODV.

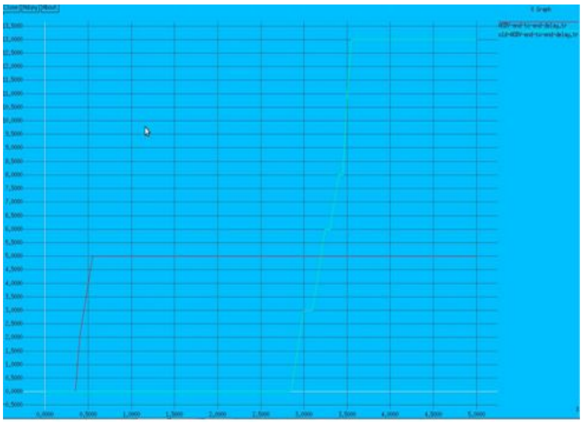

Fig.5.3 Delay

Delay graph represents that old AODV has more delay than new AODV. Thus transmission is fast in new AODV which helps to improve performance. Red line represents new AODV and green line represents old AODV.

6. Conclusion

AODV is used to find out the path of the data transfer. But simple AODV has the problem when the nodes move. Enhancement in AODV is required so that to overcome the problem of link failure during data transfer from host to destination. First of all mutual authentication is required between the mobile nodes to prevent the various inside and outside attacks. When the mobile nodes are mutually authenticated, it leads to the reliable data transmission between the mobile nodes. But the main problem occurs during the failure of the link. Due to link failure packet is lost easily. In proposed work, enhancement in AODV concept is important. This protocol is designed to provide best path according to energy. The path which has maximum energy will choose as a final path. This work will helps to reduce the problem occur in link failure and packet lost problem. Now the performance degradation problem will also improve. In new AODV, route selection is based upon the signal strength. The maximum signal strength nodes are considered as final routes.

References

[1]A. Samuel Chellathuri, E. D. (2013). "EZRP: Evolutionary Zone Routing Protocol". *ICACCS* , 1-5.

[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] Asha Ambaikar, H.R. Sharma, V. K. Mohabey , " Improved AODV for Solving Link Failure In Manet" , International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012 1 ISSN 2229-5518 2012

[5] Sunil Kumar and Pankaj Negi , "A Link Failure Solution in Mobile Adhoc Network through Backward AODV (B-AODV)", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893, 2011

[6] Ginni Tonk, I. K. (June,2012). "Performance Comparison Of Ad-Hoc Network Routing Protocols Using NS2". *IJITEE* , 53-57.

[7] Jaydip Sen, H. R. (2007). "A Mechanism for Detection of GRAY Hole Attack in Moile Ad-Hoc Network". *ICICS* , 1-5.

[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] Zaiba Ishrat, P. s. (2013). "Performance Evaluation Of DSDV, DSR and ZRP pROTOCOL in MANET". *IJCAT* , 345-349.