INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue5)

Available online at: www.Ijariit.com

Review on Rank Base Data Routing Scheme with Grey Hole Detection & Prevention in MANETS

Reena Kumari[1], Neha Goyal[2]

[1](Electronics & Communication, Desh Bhagat University, Mandi Gobindgarh

Email: reena.kumari0910@gmail.com)

[2] (Electronics & Communication, Desh Bhagat University, Mandi Gobindgarh

Email: kashish_friend_2006@yahoo.co.in)

Abstract: - MANET (Mobile Ad Hoc Network) is a type of ad hoc network that can change locations and configure itself, because of moving of nodes. As MANETs are mobile in nature, they use wireless connections to connect various networks without infrastructure or any centralized administration. While the nodes communicate with each other, they assist by forwarding data packets to other nodes in the network. Thus the nodes discover a path to the destination node using routing protocols. Gray hole attack among the different types of attacks possible in a MANET. Gray Hole attack is one type of active attack which tends to drop the packets during transmission the routing from source to destination .In this paper, we simulate gray hole attack Detection and prevention technique using AODV and AODV+PSO. Performance metrics Packet dropped or packet loss, End to End delay and Average throughput, the performance analysis has been done by using simulation tool ns-2 which is the main infrastructure.

.

Keywords – AODV, Grey hole, MANET, PSO.

1. INTRODUCTION

An ad-hoc net is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. In the absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, a wireless ad hoc network with mobile nodes as a MANET discussed here. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., mobile nodes can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes. MANET is a mobile multi-hop which is wireless distributed network and self organized in nature. The primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes. In MANET, constantly changing network topology causes link breakage and invalidation of end-to-end route.

There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols .Mobile Ad-hoc Networks (MANETs) are infrastructure less networks with distributed operations. Every node in MANET is free to enter or leave the network. In MANET all terminals are autonomous and use multi hop routing. In MANET mostly the nodes have low battery and small memory. As there is no central authority or access point in MANET, routing is very crucial issue. Research is going on to overcome all such issues. Out of these we are focusing more on security attacks in this paper. In this paper firstly we have discuss why MANET is more disposed to security attack and what different types of attacks known till. Then we have discussed the available preventive measures.

1.1 TYPES OF MANETs

1.1.1 **Infrastructure Networks**

In infrastructure based network, communication is takes place only between the wireless nodes and the access points. The communication is not directly takes place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks.

1.1.2 **Ad hoc network**

The ad hoc network is a decentralized type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. The ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it's a network which is used in urgent situation causes. There is no fixed infrastructure is required in ad hoc network like base stations. Nodes within each other radio range communicate wireless links directly.

1.2 **APPLICATION OF MANETs**

Ad-hoc networking can be applicable anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows us the device to maintain connections to the network as well as easily adding and removing devices to and from the network. MANET can be applied to a large variety of use cases where conventional networking cannot be applied. MANET is used in following areas

i) Military battlefield

The modern digital battlefield demands robust and reliable communication in many forms. In the battlefield it is needed by soldiers for relaying information related to situational awareness.

ii) Sensor Networks

Another application of MANETs is sensor networks. This technology is a network composed of a very large number of small sensors. These can be used to detect any number properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. Applications are the measurement of ground humidity for agriculture, forecast of earthquakes. The capabilities of each sensors are very limited, and each must rely on others in order to forward data to a central computer.

iii) Disaster Area Network

Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of

a communication network is needed. Information is relayed from one rescue team member to another over a small handheld.

iv) Personal Area Network:

Personal Area Networks (PANs) are formed between various mobile devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices, at home, for example, but PANs will become more meaningful when connected to a larger network.

1.3 **LIMITATIONS OF MANET**

i) Bandwidth Constraints:

The efficiency of the wireless links are always much lower than in wired counterparts. Practically, various Gbps are available for wired LAN, while, presently, the commercial applications for wireless LANs work typically around 2 Mbps.

ii) Processing capability:

Most of the nodes of the AND are devices without a powerful CPU. Furthermore, the network tasks such as routing and data transmission cannot consume the power resources of the devices, intended to play any other role, such as sensing functions.

iii) Energy constraints:

The power of the batteries is limited in all the devices, which does not allow infinitive operation time for the nodes.

iv) High Latency:

In an energy conserving design nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake up.

v) Transmission Errors:

Attenuation and interferences are other effects of the wireless link that increase the error rate.

vi) Security:

Analyses some of the vulnerabilities and attacks MANET can suffer. The authors divide the possible attacks in passive ones, when the attacker only attempts to discover valuable information by listening to the routing traffic; and active attacks, which occur when the attacker injects arbitrary packets into the network with some proposal like disabling the network.

vii) Location:

The addressing is the another problem for the network layer in MANET, since the information about the location the IP addressing used in the fixed networks offers some facilities for routing that cannot be applied in MANET. The way of addressing in MANET has nothing to do with the position of the node.

viii) Roaming:

The continuous changes in the network connectivity graph involve that the roaming algorithms of the fixed network are not applicable in MANET, because they are based on the existence of guaranteed paths to some destination.

ix) Commercially Unavailable:

MANET is yet far from being deployed on large-scale commercial basis

CONCLUSION

A conclusion section must be included and should indicate clearly the advantages, limitations, and possible applications of the paper. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications.

REFERENCES

[1] Bo Sun, Yong Guan, Jian Chen and Udo W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", In the Proceedings of European Personal and Mobile Communications Conference, pp. 490-495,2003.

[2] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks". In the Proceedings of the 42nd Annual Southeast Regional Conference, ACMSE , pp. 96-97, 2004.

[3] Pradeep Kyasanur, and Nitin H. Vaidya "Selfish MAC Layer Misbehavior in Wireless Networks", IEEE Transactions on Mobile Computing Journal, Vol. 4(5), pp. 502-516, 2005.

[4] Gao Xiaopeng, and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", In the Proceedings of IFIP International Conference on Network and Parallel Computing, pp. 209-214, 2007.

[5] R.A. Raja Mahmood and A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-Based Mobile Ad Hoc Networks", In the Proceedings of IEEE International Symposium on High Capacity Optical Networks and Enabling Technologies, pp. 1-6, 2007.

[6] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato, " A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Vol. 58(5), pp.2471 –2481, 2009.

[8] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", In the Proceedings of the 42nd Annual Southeast Regional Conference. ACM, pp. 96-97, 2004.

[9] Onkar V. Chandure and V. T. Gaikwad, "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV Routing Protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 2(6), pp. 2607-2613, 2011.

[10]Chetan S. Dhamande and H.R. Deshmukh ," A Efficient Way to Minimize the Impact of Gray Hole Attack in Ad-hoc Network", International Journal of Emerging Technology and Advanced Engineering, Vol. 2(2), pp. 106-110, 2012.

