INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue2)

Available online at: www.ijariit.com

Survey on Different Approaches of Detection of Gray Hole Attack in MANET

Geetanjali
Electronics and Communication & HPTU
Gitanjalichauhan47@gmail.com

Jyoti Gupta
Faculty of Electronics and communication &HPTU
Gitanjalichauhan47@gmail.com

Abstract: The fundamental problems of ad hoc network by giving its related research background including the concept, features, status, and vulnerabilities of MANET. They also present an overview and the study of the routing protocols. Also include the several challenging issues, emerging application and the future trends of MANET.As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. In this paper review the different technology of MANET.

Keywords: MANET, WSN Communication, ad-hoc network.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have become important in increasingly large range of applications, such as disaster recovery, rescue mission, tactical battlefield, mining operations, maritime communications, vehicle network, casual meeting, and campus network and so on. A Mobile ad hoc network (MANET) is a self-organized system which doesn't have any pre-defined network infrastructure where mobile devices are connected by wireless links. Hence, a MANET can be constructed quickly at a low cost, as it doesn't rely on existing network infrastructure. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an infrastructure less network [1]. The configuration required in network deployment is minimal where the individual node acts as routers. In an ordinary wireless network, two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multi-hop. A communication session is achieved either through single-hop transmission if the recipient is within the transmission range of the source node, or by relaying through intermediate nodes otherwise.

Mobile Ad hoc Network (MANET) is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. Theses nodes can act as both routers and hosts. Those have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topology are used [2]. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behaviour easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic [3].

An ad-hoc network 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 [4].

As MANETs are illustrate by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes, topology changes and unreliable communication in the design. There are many types of protocol are available in MANET. Its efficiency of a routing protocol is determined by its battery power consumption of a participating node and routing of traffic into the network [5].

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 [6]. 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 [7].

Types of MANET [12]

Wireless Networks term is refers to a kind of networking that does not require cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level. It is also known as Wi-Fi or WLAN. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information. The IEEE standard for wireless network is 802.11.

There are two types of Wireless Operating modes:

- **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.
- **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 [9]. There is no fixed infrastructure is required in ad hoc network like base stations. Nodes within each other radio range communicate wireless links directly [6].

II. LITERATURE REVIEW

Goyal et. Al [1], described the fundamental problems of ad hoc network by giving its related research background including the concept, features, status, and vulnerabilities of MANET. They also present an overview and the study of the routing protocols. Also include the several challenging issues, emerging application and the future trends of MANET.As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to severe challenges, the special features of MANET bring this technology great opportunistic together.

Wahane & Lonare [3], proposed an Algorithm to detect cooperative Black Hole Attack and examination has been done by considering three different cases. In the first case there were no malicious node present in the network and the reply for route request was from the reliable node so based on this previous information of reliability of node the route is confirmed to be secured. In the second case there were two Black Hole nodes in the network mutually cooperating with each other as there was no previous information for these two nodes so they are checked for reliability and found malicious at the end and this information of malicious behaviour was propagated throughout the network. In the third case a node is found to be reliable and this information is broadcasted throughout the network and third bit with respect to that node is set to true which shows that the node in question is trustful node. Finally it has been concluded that this algorithm works well in all the three cases with the aim of detecting Cooperating Black Hole Attack and ensuring a secure as well as reliable route from source to destination. It also decreases routing overhead and end to end delay.

Wadbude and Richariya [4], discussed about an ad-hoc network is a multi-hop wireless network where all nodes cooperatively maintain network connectivity without a centralized infrastructure. If these nodes change their positions dynamically, it is called a mobile ad-hoc network (MANET). Since the network topology changes frequently, efficient adaptive routing protocols such as AODV, DSR are used. As the network is wireless, security becomes the major issue in MANETs. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehaviour of malicious nodes, which disrupts the transmission. Here proposed an efficient secure AODV routing protocol. Simulation results show that proposed routing algorithm provides a better level of security and performance than existing works. The simulation results show the improvement of the network performance, in terms of overhead, and end to end delay to the secure AODV routing protocol.

Sharma and Singh [6], proposed sequenced queue based routing algorithm for detection and correction of gray-hole attack by implementing intrusion detection system. In future work new algorithm based on trace gray and course based algorithm proposed and Improve gray-hole detection rate and reduce network load.

Chen et. al [8], discussed about importance of mutual authentication for wireless sensor networks .Here also discussed about the DES protocol which is the hash-based authentication protocol. This protocol provides the security aligned with the stolen-verifier, masquerade, replay, and guessing attacks.

Raj and Swadas [9], proposed a new control packet called ALARM is used in DPRAODV while other main concepts are dynamic threshold value. Unlike normal AODV, the RREP_seq_no is extra checked whether higher than the threshold value or not. If the value of RREP_seq_no is higher than the threshold value, the sender is regarded as an attacker and updated it to the black list. The ALARM is sent to its neighbours who includes the black list, thus the RREP from the malicious node is blocked but is not processed. On the other hand, the dynamic threshold value is changed by calculating the average of dest_seq_no between the sequence number and RREP packet in each time slot. According to this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment. In the simulation results, the packet delivery ratio is improved by 80-85% than AODV when under black hole attack, and 60% when traffic load increases. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV, except for it takes a little bit higher routing overhead and end-to-end delay. But DPRAODV simply detects multiple black holes rather than cooperative black hole attack.

Yi and Kravets [10], discussed various mutual authentication schemes of MANET and symmetric key and asymmetric key distribution schemes. In this they also discuss PKI (public key distribution) scheme which based on the symmetric key distribution scheme. In new authentication scheme had been proposed named as MOCA, in which hybrid type of scheme, both PKI and asymmetric schemes used for mutual authentication.

Deng et. al [11], proposed a technique for detecting a chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc networks. In order to detect gray whole attack the total traffic volume is divided into a set of small data blocks. Initially a backbone network of strong nodes is built by this technique over the ad hoc network. These strong nodes are assumed to be powerful in terms of computing power and radio ranges. Also each strong node is assumed to be a trustful one. Nodes are considered as a strong node otherwise ordinary node. The major drawback of this approach is the assumption that some strong nodes which are powerful in terms of power and antenna range are available in the network. The optimality of backbone network is not proved in terms of minimality and coverage. The assumption that strong nodes are always trusted node will fail if the intruder attacks strong nodes.

Al-Shurman et. al [12], presented two possible solutions for the black hole problem which is one of the security attacks that occur in mobile ad hoc networks (MANETs). The first is to find more than one route to the destination. The second is to exploit the packet sequence number included in any packet header. Their computer simulation shows that compared to the original ad hoc on-demand distance vector (AODV) routing scheme; the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.

CONCLUSION

In this paper we detect the gray hole attack by checking of fake reply in the network, in this paper work we check the route of the network in which data is transmit from source to destination. It check the probability of the malicious node which are present in network, by probability check we can detect the malicious node. With future emphasis given for the secure transmission, we can prevent the MANET by malicious node using different methodology.

REFERNCES

1. Priyanka Goyal, Vintra Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", International Journal of Computational Engineering & Management, Vol. 11, pg. 32-37, 2011.
2. Sevil Şen, John A. Clark and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks Auerbach Publications", pp. 1-20, 2011.
3. Gayatri Wahane and Savita Lonare, "Technique for Detection of Cooperative Black Hole Attack in MANET", Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, pp. 1-8. IEEE, 2013.
4. Durgesh Wadbude and Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology, Vol. 1(4), pp. 274-279, 2012.
5. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Journal-Communications Network, Vol. 3(3), pp. 60-66, 2004.
6. Shivani Sharma and Tanu Preet Singh, "Sequenced Queue Based Routing Algorithm (SQRA) for Detection and Correction of Gray Hole Attack by Implementing IDS", In the Proceedings of the International Conference on Recent Trends In Computing and Communication Engineering, pp.43-47, 2013.
7. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer Journal of Wireless Mobile Network Security, pp. 103-135, 2006.
8. Tien-Ho Chen and Wei-Kuan and Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks", Electronics and Telecommunications Research Institute (ETRI) Journal , Vol 32(5), pp. 704-712, 2010.
9. Payal N. Raj and Prashant B. Swadas, "DPRAODV: A Dynamic Learning System Against Black hole Attack In AODV Based MANET", International Journal of Computer Science Issues (IJCSI), Vol. 2, pp. 54–59, 2009.
10. Seung Yi and Robin Kravets, "Key Management for Heterogeneous Ad-Hoc Wireless Networks", In the Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 1092-1648, 2002.
11. Hongmei Deng, Wei Li and Dharma P. Agrawal, "Routing Security in Wireless Ad hoc Networks", IEEE Communications Magazine Journal, Vol. 40(10), pp. 70-75, Oct. 2002.
12. 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.

