Review: Blackhole Attack Detection on MANET

Shweta Pandey[1], Mr. Varun Singh[2]

[1]M.Tech Scholar, [2]Assistant Professor

Department of Computer Science, Rewa Institute of Technology, Rewa, India

Abstract:Mobile Ad-hoc Network (MANET) consists of different ways of configuration in which it deals with the dynamic nature for its creation and also it is a self-configurable type of a network. This network can be usedtemporarily as it doesn't have any centralised control. So, because of its flexible nature, it suffers from various attacks. The primary task in this type of networks is to develop a mechanism for routing that gives a high QoS parameter because of nature this ad-hoc network. The task done in this paper is to design a routing mechanism for security by using the Ad-hocOn-Demand Distance Vector (AODV) protocol. The AODV we use here is the on-demand routing mechanism for the computation of the trust, which is used for the path selection. Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. In this paper, we focus on Black Hole attack in Mobile adhoc networks. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solution are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. MANET can operate in isolation or in coordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. This flexibility, along with their self organizing capabilities, are some of MANET's biggest strengths, as well as their biggest security weaknesses. In this paper different routing attacks, such as active(flooding, black hole, spoofing, wormhole) and passive(eavesdropping, traffic monitoring, traffic analysis) are described.

Key Words:Mobile Ad hoc Network, Support Vector Model, AODV, Artificial Neural Network, Blackhole Attack(BA).

I. INTRODUCTION

Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks, where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in an intimate manner to engaging themselves in multihop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transferring packets; so there is need of a routing procedure. This is always ready to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

1.1 Properties of Ad-Hoc Routing Protocols Properties of Ad-Hoc Routing Protocols

The properties that are desirable in Ad-Hoc Routing protocols are :

Distributed operation The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The dissimilarity is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.

Loop free: To improve the overall performance, the routing protocol should assurance that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

Demand based operation To minimize the control overhead in the network and thus not misuse the network resources the protocol should be reactive. This means that the protocol should react only when needed and should not periodically broadcast control information.

Unidirectional link support The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

Security : The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.

Power conservation The nodes in the ad-hoc network can be laptops and thin clients such as PDA_s that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

Multiple routes To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

Quality of Service Support Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support.

II. LITERATURE SURVEY

[1]Mrs.Padma .P, et.al.,Mobile Ad-hoc Networks (MANET) is an emerging area of research. Most current work is centered with different issues. This paper discusses the issues associated with data communication with MANET, Security in MANET, Intrusion detection. A mobile adhoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Adhoc Network usually seek the help of other intermediate nodes to establish communication channels. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. In this paper we also focus on Intrusion detection system(IDS) and also tried to elaborate on security attacks, IDS architectures, and different intrusion detection mechanisms.

[2]KUTHADI VENU MADHAV , et.al.,Wireless Sensor Networks (WSN) is a recent advanced technology of computer networks and electronics. The WSN increasingly becoming more practicable solution to many challenging applications. The sensor networks depend upon the sensed data, which may depend upon the application. One of the major applications of the sensor networks is in military. So security is the greatest concern to deploy sensor network such hostile unattended environments, monitoring real world applications. But the limitations and inherent constraints of the sensor nodes does not support the existing traditional security mechanisms in WSN. Now the present research is mainly concentrated on providing security mechanism in sensor networks. In this context, we analysis security aspects of the sensor networks like requirements, classifications, and type of attacks etc., in this survey paper.

[3]Deepika Kukreja, et.al.,A mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. Due to lack of centralized control, dynamic network topology and multihop communications, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security in infrastructure based networks. Several protocols for secure routing in ad hoc networks have been proposed in the literature. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks. This paper presents a survey of trust based secure routing protocols for mobile ad hoc networks. Different trust based secure routing protocols are discussed and analyzed in the paper along with their strengths, weaknesses and future enhancements.

[4]G.S. Mamatha, et.al., The foremost concerned security issue in mobile ad hoc networks is to protect the network layer from malicious attacks, thereby identifying and preventing malicious nodes. A unified security solution is in very much need for such networks to protect both route and data forwarding operations in the network layer. Without any appropriate security solution, the malicious nodes in the network can readily act to function as routers. This will solely disturb the network operation from correct delivering of the packets, like the malicious nodes can give stale routing updates or drop all the packets passing through them. In this paper a study that will through light on such attacks in MANETS is presented. The paper also focuses on different security aspects of network layer and discusses the effect of the attacks in detail through a survey of approaches used for security purpose.

III. SECURITY ATTACKS

Securing wireless adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET.

3.1 These attacks can be classified into two types:

3.1.1 Passive Attacks Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

3.1.2 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 involve some modification of data stream or creation of false stream. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication.

3.2 Active Attacks

The following are the various Active Attacks in MANET:

3.2.1 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 that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packet that it receive instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

3.2.2 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. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole .In DSR,AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network.

3.2.3 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 which results in disruption or degradation of routing services within the network.

3.2.4 Rushing attack Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

3.3 PASSIVE ATTACKS

3.3.1 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, other wireless network such as cellular, satellite and WLAN also suffer from these potential vulnerabilities.

3.3.2 Eavesdropping The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.

3.3.3 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.

3.3.4 Syn flooding This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

3.4 What Is Black Hole ? Black hole is one of many attacks that take place in MANET and is considered as one of the most common attacks made against the AODV routing protocol. The black hole attack involves malicious node pretending to have the shortest and freshest route to the destination by constructing false sequence number [3] in control messages. AODV protocol was created without any security considerations [4]. Thus, no protection mechanism was built to detect the existence of malicious attack. In the AODV, maintaining a fresh route to ensure safe path to destination is very vital due to the rapid change of the network topology. The manipulation done by the malicious node will deny the genuine Route Reply (RREP) message from other nodes especially the reply message coming from the actual destination node.

3.5 Black Hole Detection and Prevention Techniques

DPRAODV(Detection,Prevention and Reactive AODV) scheme In this paper authors proposed have proposed the method DPRAODV (A dynamic learning system against black hole attack in AODV based MANET) to prevent security of black hole by informing other nodes in the network. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbors. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

ABM (Anti-Blackhole Mechanism) scheme This paper attempts to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Blackhole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node.

Honeypot based detection scheme Authors propose a novel strategy by employing mobile honeypot agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements. We collect valuable information on attacker's strategy from the intrusion logs gathered at a given honeypot.

ERDA (Enhance Route Discovery for AODV) scheme Have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. a method called ERDA (Enhance Route Discovery for AODV). The proposed method is able to mitigate the a foresaid problem by introducing new conditions in the routing table update process and also by adding simple malicious node detection and isolation process to the AODV route discovery mechanism. The proposed method does not introduce any additional control message and moreover, it does not change the existing protocol scheme.

Cryptographic based technique This paper focuses that many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability. These techniques cannot prevent a malicious node from dropping packets supposed to be relayed, There are basically three defense lines devised here to protect MANETs against the packet dropping attack. The first defense line (for prevention purposes) aims to forbid the malicious nodes from participating in packet Forwarding function. Whenever the malicious node exceeds this barrier, a second defense line (for incentive purposes) is launched, which seeks to stimulate the cooperation among the router nodes via an economic model. Finally, once the two previous defense lines have been broken, a third on (for detection/reaction purposes) is launched aiming to reveal the identity of the malicious node and excludes it from the network.

IV. CONCLUSION

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. Various types of Black Hole detection and Prevention techniques has been discussed in this paper. It has been also be discussed that the MANET must provide a mechanism to prevent the black hole attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The research on MANET security is still in its early stage. Therefore, a more ambitious goal for ad hoc network security is to develop a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many both known and unknown security threats.

REFERENCES

[1] Dr.S.S.Dhenakaran, A.Parvathavarthini ,An Overview of Routing Protocols in Mobile Ad-Hoc Network

[2] G. Murali, D. Pavan, V.V. Rajesh Reddy, P. Bharath kumar, DYNAMIC ROUTING WITH SECURITY CONSIDERATIONS

[3] K.V.S.Mounika, Nanduri Jyothirmai, A.Rama Krishna ,Dynamic Routing With Security Considerations

[4] Navid Nikaein, Houda Labiod and Christian Bonnet ,DDR-Distributed Dynamic Routing Algorithm for Mobile Ad hoc Networks

[5] K. S. Arathy and C. N. Sminesh, "A Novel Approach for Detection of Single and Collaborative Blackhole Attacks

in MANET," Procedia Technology, vol. 25, pp. 264-271, 2016.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[6] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad Hoc Networks," in International Conference on Wireless Networks, Icwn '03, June 23 - 26, 2003, Las Vegas, Nevada, Usa, 2003, pp. 570-575

[7] V. Khandelwal and D. Goyal, "Blackhole Attack and Detection Method for AODV Routing Protocol in MANETs," International Journal of Advanced Research in Computer Engineering & Technology, vol. 2, 2013.

[8] S. Kumar, D. Singh and S. Chandra, "Analysis and Implementation of AODV Routing Protocol against Blackhole Attack in MANET," International Journal of Computer Applications, vol. 124, pp. 975-8887, 2015.

[9] S. Sharma and R. Gupta, "SIMULATION STUDY OF BLACKHOLE ATTACK IN THE MOBILE AD HOC NETWORKS," Journal of Engineering Science & Technology, vol. 4, 2009.

[10] S. Dokurer, Y. M. Erten and C. E. Acar, "Performance analysis of ad-hoc networks under Blackhole Attacks," in IEEE Southeastcon, 2007, pp. 148-153.

[11] C. G. Ma and J. S. Yao, NS-3 Network Simulator Basics and Applications: Posts & Telecom Press, 2014, pp.1-12.

[12] N. Purohit, R. Sinha and K. Maurya, "Simulation study of Blackhole and Jellyfish attack on MANET using NS3," in Nirma University International Conference on Engineering, 2012, pp. 1-5.

[13] M. Al-Shurman, S. M. Yoo and S. Park, "Blackhole Attack in mobile Ad Hoc networks," in Southeast Regional Conference, 2004, pp. 96-97.

[14] F. H. Tseng, L. D. Chou and H. C. Chao, "A survey of Blackhole Attacks in wireless mobile ad hoc networks," Human-centric Computing and Information Sciences, vol. 1, p. 4, 2011.

[15] G. Li, Z. Yan and Y. Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network," 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, 2018, pp. 1-6, doi: 10.1109/CNS.2018.8433148.