International Journal of Computer Applications Technology and Research
Volume 3– Issue 6, 374 - 376, 2014

Detection of Black Hole in AD- HOC Networks

Sona Malhotra
UIET
Kurukshetra, Haryana
India

Sandeep Kumar
UIET
Kurukshetra, Haryana
India

ABSTRACT: Unattended installation of sensor nodes in the environment causes many security threats in the Ad-hoc networks. The security of the DSR protocol is threaded by a particular type of attack called Black Hole attack. Black hole in Ad- hoc networks is a major problem. The proposed work includes detection and countermeasure rules to make the sensor network secure from these attacks. In our research DSR routing protocol is used to detect which node sends the reply after getting the request packet. This work will lead to minimum delay of packets in simulation results.

Keywords: Ad-hoc network, Black hole, routing protocol, DSR.

1. INTRODUCTION

Ad-hoc networks are a collection of thousands of nodes that are small in size, cheaper in price with restricted energy storage, less memory space and limited processing capability. Ad-hoc networks are mobile wireless networks that have no fixed infrastructure. There are no fixed routers instead each node acts as a router and forwards traffic from other nodes. Ad hoc networks are a new paradigm of wireless communication for mobile hosts which are also known as nodes.This network allow spontaneous formation and deformation of mobile networks. A mobile ad hoc network is a collection of mobile hosts that communicates with each other within the network. MANET has Multi-hop commutation capability. There is no defined administration or a backbone network to support it. In these types of networks each node works as an independent router. Each mobile host use wireless RF transceivers as network interface.

1.1 Security Attributes

- Availability: ensures the survivability of network services despite denial of service attacks. A denial of service attack can be launched at any layer of an ad hoc network. On the physical and media access control layers an adversary node employ jamming to interfere with communication on physical channels. On the network layer, an adversary node could destroy the routing protocol and disconnect the network. On the higher layers an adversary node could bring down high-level services.
- Authentication: enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary node could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.
- Non-repudiation: ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.
- Confidentiality: Ensures that secret information or data is never disclosed to unauthorized devices. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.
- Integrity: Ensures that a message received is not corrupted. A message could be corrupted because of benign failures such as radio propagation impairment or because of malicious attacks on the network.

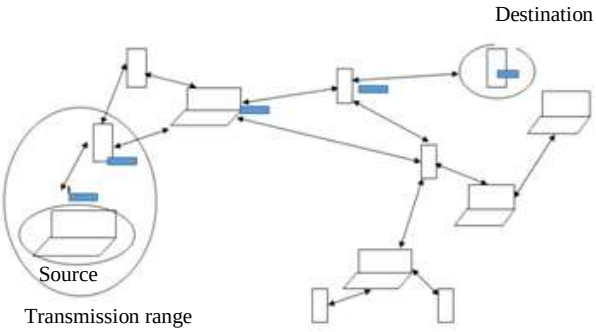

Figure 1.1 Data transmission in Ad-hoc network

1.2 Types of attacks

Black hole attack: The Black hole is a kind of denial of service where a malicious node can attract all other packets by falsely claiming a fresh route to the destination and then absorb them without forwarding. [1][2]. Cooperative Black hole means the malicious node acts in a group. A black hole attack can be easily launched by an adversary node in the sensor network. The Black hole attack is an active insider attack. Since the data packets do not reach the destination node on account of this attack data loss will occur. It has two properties: first the attacker consumes the diverted packets without any forwarding to the receiver. Second the nodes destroy the mobile ad hoc routing protocol to promote itself as it is having a valid route to a destination node. The defected node tried to advertise itself about the path of the route to the destination node.

Gray hole Attack: The attacker node initially forwards the packets and participates in routing. The Gray Hole node advertises itself as having a valid or shortest path to the destination node initially. A Gray Hole may exhibit its malicious behaviour in various techniques. It simply drops packets coming from or destined to certain specific nodes in the network while forwarding all the packets for other nodes[3].

1.2 Protocol Used

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks. DSR allows the network to be completely self-organizing and self-configuring without the need for any existing network infrastructure or administration. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes and is designed to work well even with very high rates of mobility. This document specifies the operation of the DSR protocol for routing unicast IPv4 packets. In DSR every mobile node in the network needs to maintain a route cache where it caches source routes that it has learned. When a host wants to send a packet to some other host it first checks its route cache for a source route to the destination. In the case a route is found the sender uses this route to propagate the packet. Otherwise the source node initiates the route discovery process. Route discovery and route maintenance are the two major parts of the DSR protocol.

2. RELATED WORK

1. Leela Krishna Bysani *et al.* [4] suggested that WSN will emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks since once deployed these networks were unattended and unprotected. Some of the inherent features like limited battery and low memory makes sensor networks infeasible to use conventional security solutions which needs complex computations and high memory. There were lot of attacks on these networks which can be classified as routing attacks and data traffic attacks. Some of the data attacks in sensor nodes are wormhole, black hole and selective forwarding attack. In a black hole attack, compromised node drops all the packets forwarding through it. A special case of black hole attack was selective forwarding attack where compromised node drops packets selectively which may deteriorate the network efficiency. In this paper the author discussed about selective forwarding attack and some of the mitigation schemes to defend this attack.
2. Jatin D. Parmar *et al.* described that Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore interest in research of Mobile Ad-hoc Network has been growing since last few years. In this paper the author have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security was a big issue in MANETs as they were infrastructure-less and autonomous. Main objective of writing this paper was to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. This article would be a great help for the people conducting research on real world problems in MANET security.
3. Sukla Banerjee *et al.* [31] proposed an algorithm for detection & removal of Black/Gray Holes. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks in the hope that the malicious nodes can be detected & removed in between transmission. Flow of traffic was monitored by the neighbors of each node. Source node uses the acknowledgement sent by the destination to check for data loss & in turn evaluates the possibility of a black hole. However in this mechanism false positives may occur and the algorithm may report that a node is misbehaving.
4. Sarvesh Tanwar *et al.* [1] suggested that with the advancement in radio technologies like Bluetooth IEEE 802.11 a new concept of networking has emerged; this was known as ad hoc networking where potential mobile users arrive within the range for communication. As network was becoming an increasingly important technology for both military and commercial distributed and group based applications, security was an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks MANETs were more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks or internal attack and external attacks the security services such as confidentiality, authenticity and data integrity were also necessary for both wired and wireless networks to protect basic applications. One main challenge in design of these networks were their vulnerability to security attacks. In this paper the author study the threats an ad hoc network faces and the security goals to be achieved.
5. Sonia *et al.* [2] proposed that due to the spontaneous nature of ad-hoc networks, they were frequently established insecure environments, which made them vulnerable to attacks. These attacks were launched by participating malicious nodes against different network services. Ad hoc On-demand Distance Vector routing (AODV) was broadly accepted network routing protocol for Mobile Ad hoc Network (MANET). Black hole attack was one of the severe security threats in ad-hoc networks which could be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV. In this paper a review on different existing techniques for detection of pooled or co-operated black hole attacks with their defects were presented.
6. Fidel Thachil *et al.* [3] presented a trust based collaborative approach to mitigate black hole nodes in AODV protocol for MANET. In this approach every node monitors neighbouring nodes and calculates trust value on its neighbouring nodes dynamically. If the trust value of a monitored node goes below a predefined threshold, then the monitoring node assume it as malicious and avoids that node from the route path. The experiment reveal that the proposed scheme secures the AODV routing protocol for MANET by mitigating and avoiding black hole nodes.

3. PROPOSED WORK

The proposed work will check the percentage of packets received. This will combat black hole in DSR routing protocol. In this approach any node uses number rules to inference about honesty of reply's sender. The main aim is to check out the set of malicious nodes locally at each node

whenever they tries to act as a source node. The network will wait and check the replies from all neighbouring nodes to find a safe route. The performance is measured in terms of packet delivery then DSR (Dynamic source Routing Protocol) in the presence of black holes with minimum delay. The use of dynamic source routing is it allows packet routing to be loop-free. It does not require any up-to-date routing information in the intermediate nodes through which packets are forwarded. The Simulation's results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional DSR in the presence of Black holes with minimal additional delay and Overhead.

4. CONCLUSION

In this paper, we discuss the security issues in a MANET related to black hole attack. This type of attack can be easily deployed in MANET. The black hole node may be single or it may form a co-operative black hole attack. The solution provided in this paper is simulated using a simulator created in java and it demonstrated the detection of black hole attacks in MANET. Once a black hole is detected the node last sending the data packet, stores in it the information about the black hole, so that it doesn't interact with black hole again. Future works can be concentrated on ways to propagate the information about the black hole in the entire network so as to isolate the attacking node.

5. REFERENCES

1. Leela Krishna Bysani and Ashok Kumar Turuk "A Survey On Selective Forwarding Attack in Wireless Sensor Networks" International conference on devices and communications, February, 2011
2. Jatin D. Parmar, Ashish D. Patel, Rutvij H.Jhaveri and Bhavin I. Shah "MANET Routing Protocols and Wormhole Attack against AODV" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010
3. Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008
4. SarveshTanwar, Prema K.V. "Threats & Security Issues in Ad hoc network: A Survey Report" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013
5. Sonia and Abhishek Aggarwal "A Review Paper on Pooled Black Hole Attack in MANET"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013
6. Fidel Thachil and K C Shet "A trust based approach for AODV protocol to mitigate black hole attack in MANET" International Conference on Computing Sciences, 2012