PREVENTION OF BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORK USING INTRUSION DETECTION SYSTEM

Abhishek Mishra, Mohsin Shah, Ankush Gore, Moreshwar Pidadi, Ravindra Hirulkar

Final Year B.Tech, Information Technology, Government College of Engineering Amravati, Maharashtra, India, ***abhishek.mishra1707@gmail.com***
Final Year B.Tech, Information Technology, Government College of Engineering Amravati, Maharashtra, India, ***mohsin7827@gmail.com***
Final Year B.Tech, Information Technology, Government College of Engineering Amravati, Maharashtra, India, ***gore.ankush007@gmail.com***
Final Year B.Tech, Information Technology, Government College of Engineering Amravati, Maharashtra, India, ***moreshwarpidadi@gmail.com***
Final Year B.Tech, Information Technology, Government College of Engineering Amravati, Maharashtra, India, ***ravishirulkar@gmail.com***

Abstract

A Mobile ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. In this paper, we simulated the black hole attack in mobile ad-hoc network and have tried to find a response system in simulations.

Keywords: Mobile Ad-hoc Network, Black Hole Attack, Simulation, Security, Intrusion Detection Systems.

---------- *** ----------

1. INTRODUCTION:

As mobile ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbour nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. In our study, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Black Hole attacks, we first added a new Black Hole protocol into the NS-2. We started our project by adding a new AODV protocol using C++, to simulate the Black Hole attack. Having implemented a new routing protocol which simulates the black hole we performed tests on different topologies to compare the network performance with and without black holes in the network. Afterwards, we proposed an IDS solution to eliminate the Black Hole effects in the AODV network.

2. SECURITY ISSUES FOR MANETs:

Vulnerabilities of operating systems and upper layer applications that belong to user programs such as databases, browsers or client-server applications are not considered as a security issue for mobile ad-hoc networks. General attack

types are the threats against the routing layer of the mobile ad-hoc networks; such as physical, MAC and network layer which is the most important function of mobile ad-hoc network for the routing mechanism, orienting the packets after a route discovery process. Attacks to the mobile ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. Using one of the key mechanisms such as cryptography or authentication, or both in a network, serves as a preventive approach and can be employed against '*attackers*'. However, these mechanisms protect the network against attacks that come from outside, malicious '*insiders*' which use one of the critical keys can also threaten the security. For instance, in a battle field where mobile ad-hoc networks are used, even if keys are protected by temper proof hardware that are used in the vehicles in the network, it is difficult to say that these vehicles exhibit the same behaviour if the enemy captures them. On the other hand, a node may undeliberate misbehave as if it is damaged. A node with a failed battery which is unable to perform network operations may be perceived as an attack. Another malicious behaviour of the nodes is selfishness. Selfish nodes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore; failed and selfish nodes also affect the network performance as they do not correctly process network packets, such as in routing mechanism. We should, therefore ensure that everything is correctly working in the network to support overall security and know how an insider is able to attack the mobile ad-hoc network. Mobile ad-hoc networks should be protected with an intrusion detection system that can understand the possible actions of attackers and can produce a solution against these attacks.

2.1 BLACK HOLE ATTACK:

The difference of Black Hole Attacks compared to other attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighbouring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

3. BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL:

Initially, we should take into account Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol and then we shall explain Black Hole Attack.

3.1. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL:

Ad-hoc On-Demand Distance Vector (AODV Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Because of these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for stabilising a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbours (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbours. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node. Afterwards the RREP message is unicasted to the source node. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol.

4. SOLUTION FOR BLACK HOLE ATTACK AND ITS EFFECTS:

All IDS nodes in this paper execute a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds the predefined threshold, a block message is broadcast by a nearby IDS, giving notice to all

nodes on the network to cooperatively isolate the malicious node. The Block message contains the issuing IDS, the identified black hole node, and the time of identification. Upon receipt of a Block message issued by IDS, normal nodes will place the malicious node on their blacklists, thus, the AODV routing protocol for normal nodes must be slightly revised. There are three assumptions in this paper, as follows.

Assumptions:

1. Two neighbouring IDS nodes are located within each other's transmission range in order to forward Block messages to each other.
2. An authentication mechanism exists in MANETs, wherein, a node ID cannot be forged, and a block message, sent by an IDS node, cannot be modified or counterfeited.
3. Every IDS is set in promiscuous mode in order to sniff all routing packets within its transmission range.

There are three types of nodes in the network topology of this paper, which separately perform three algorithms, as follows.

Malicious node: selectively executes the BAODV (Black hole AODV) routing algorithm for black hole attacks.

Normal node: executes a slightly revised AODV, called MAODV (Modified AODV), to conduct normal routing, and also blocks the malicious nodes in collaboration with IDS nodes.

IDS node: executes ABM (Anti-Black hole Mechanism) to detect black hole nodes, and issues a Block message, if necessary.

Generally, a malicious node behaves like a normal node, and conducts normal routing by performing MAODV (modified AODV). In the event of an attack occurrence, the malicious node turns to perform BAODV (Black hole AODV), set RREP with an extremely large sequence number, and 1 hop count in response to RREQ, which makes it possible to quickly acquire the route. When receiving data packets, BAODV will directly drop them, and generate a black hole attack. If a malicious node is detected by IDS, it will broadcast the malicious node's ID, through a Block message, to all nodes within the transmission range. When a normal node receives a Block message, the malicious node's ID is added to the Block table. And by using table data all normal nodes in mobile ad-hoc network blocks black hole node

.

5. CONCLUSION

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.

ACKNOWLEDGEMENT

We would like to express our deep and sincere gratitude to **Prof. S. A. Lohi.** His critical comments, advice and guidance have been very valuable to us. Above all, we are highly grateful for his timely, detailed corrections. We are greatly thankful for his patience, understanding and encouragement. We would also like to thank **Prof. A. V. Deorankar**, Head of the Department, Information Technology Department for providing us this opportunity to present this report. We would thank **Dr. W. Z. Gandhare**, Principal, Government College of Engineering, Amravati for providing all the facilities at the right period of time. Finally, we would like to thank all those who directly or indirectly helped us during our work.

REFERENCES

[1]. H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.

[2]. K Fall and K. Varadhan, The NS Manual, November 18,2005,http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf . 25 July 2005.

[3]. Semih Dokurer, Y.M. Erten, Can Erkin Acar, ''Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. Of the IEEE SoutheastCon, pp. 148–153, 2007.

[4]. http://www.wikipedia.com