Authentication Mechanism-Based Black Hole Attack Prevention

Divya Paikaray, Assistant Professor

Department of Computer Science, Arka Jain University, Jamshedpur, Jharkhand, India

Email Id- divya.p@arkajainuniversity.ac.in

ABSTRACT: A MANET is a new study field with real-world applications. However, because of its basic features, such as open medium, dynamic topology, dispersed collaboration, and limited capabilities, a MANET is especially susceptible. Routing is critical to the overall network's security. One of the security threats that occur in Mobile Ad-hoc Networks is the black hole attack (MANETs). A rogue node uses the routing protocol to promote itself as having the quickest route to the node whose data packets it wishes to intercept in this attack. The black hole issue is addressed in this article. On top of Ad-hoc On-demand Distance Vector, an authentication method based on the hash function, the Message Authentication Code (MAC), and the Pseudo Random Function (P RF) is suggested for black hole avoidance (AODV). The simulation results demonstrate that the method offers quick message verification, detects a black hole, and finds a safe routing path to prevent a black hole assault.

KEYWORDS: Authentication, Routing protocols, Mobile ad hoc networks, Information security, Ad hoc networks, Computer crime

1. INTRODUCTION:

A MANET is a multi-hop temporary communication network made up of mobile nodes equipped with wireless transmitters and receivers that operates without the use of existing network infrastructure. As a result, MANET activities pose additional security issues in addition to those already existing in fixed networks[1].Attacks in MANETs may be classified into two types based on whether or not attackers affect the functioning of a routing protocol. In a passive attack, the attacker does not try to disrupt the functioning of a routing protocol, but rather listens to the routing flow for useful information. In an active assault, however, adversaries undertake activities like as modifying and deleting transmitted data in order to draw packets intended for other nodes to the attacker for analysis or simply to destroy the network[2].The following are some examples of active attacks that may be readily carried out against MANETs

- Black hole: A malicious node may advertise itself as having the quickest route to the node whose packets it wishes to intercept via the routing protocol. Section 2 has a more comprehensive description.

- Denial of Service (DoS): A malicious node may send out many unnecessary routing requests in order to prevent other nodes from accessing network resources. When a hostile node hijacks network bandwidth, a DoS attack occurs.

- Impersonation: A hostile node may impersonate another node while delivering control packets in order to cause a Routing Table anomalous change (RT).

- Disclosure: A rogue node in the network may leak sensitive information, such as routing or location information, to unauthorized users. At the end of the day, the attacker knows where the nodes on the target route are.

- Spoofing happens when a node in the network misrepresents its identity, for as by changing its MAC or IP address in outgoing packets. Spoofing in combination with packet manipulation is a very hazardous combination.

- Sleep deprivation: MANETs use battery-powered devices to save energy by only transmitting when absolutely required. By demanding routings or sending unneeded traffic to the nodes, an attacker may try to drain batteries[3].

These are systems that aid in the prevention, detection, and response to security threats. In order to maintain a dependable and secure ad-hoc network environment, four key security objectives must be met. They're mostly:

- Confidentiality: The protection of any information against unintentional disclosure. Because intermediary nodes (that serve as routers) receive packets for other receivers, they may readily eavesdrop on the information being routed, this is harder to accomplish with MANETs.

- Availability: It ensures that the system's services are accessible at all times and that authorized users are not denied access.

- Authentication: Confirmation that an entity of interest or the source of a communication is who or what it claims to be. Without it, an attacker may impersonate a node and obtain unauthorized access to resources and sensitive data, as well as disrupt the functioning of other nodes.

- Message Integrity: The message is never tampered with during transmission.

- Non-repudiation: Assures that neither the sender nor the receiver can deny ever sending or receiving the communication[4].

- Assurance: It is necessary to ensure that the security measures have been correctly installed and are working as planned.

- Non-repudiation: This ensures that neither the sender nor the receiver can deny ever sending or receiving the communication[5].

The remainder of the paper is laid out as follows: The black hole attack in MANETs is addressed in section II. We provide an authentication method to avoid the black hole attack in detail in part III, followed by the simulation results in section IV. In part V, we come to a conclusion and discuss the next steps.

Attack on the Black Hole

The AODV Routing Protocol (A. AODV Routing Protocol) is a routing protocol that In MANETs, AODV is an on-demand routing mechanism. Route exploration isn't begun unless it's absolutely necessary (ondemand). Route discovery and route maintenance are the two methods that the protocol uses. When a packet sender's routing table (RT) is empty, route discovery is utilized. It sends out a RouteRequest packet to the rest of the network. When a node gets a new RouteRequest, it examines its RT to determine whether it has a route to the requested location. If there is one, it responds; if not, the RouteRequest is sent.It maintains a reverse route to the source node in its RT before forwarding. The RT saves the next hop's route information, as well as the distance and the highest sequence number it has seen so far. Route maintenance begins when a cached route becomes invalidated due to changes in the network topology. It's used to send a message to the source node or to start a new route discovery[6].

B. ADVO's Weakness

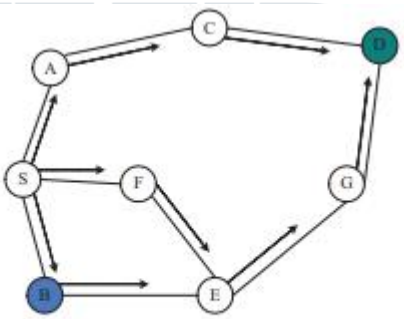
It is possible to interrupt communication between nodes by exploiting a variety of flaws in AODV. The following are some of AODV's flaws

RREQ False Message Propagation: The aim of this attack is to redirect traffic via the malicious node before discarding it. RREP False Reply: This attack intercepts a request and responds to it, ideally before it reaches its ultimate destination. RREP-based fake message propagation: In this attack, the hostile node uses false RREP packets to redirect traffic. The goal is to create a black hole and eliminate traffic. If a source node does not have a route to transmit data packets to a target node in its RT, it will start the routing discovery procedure.[7]

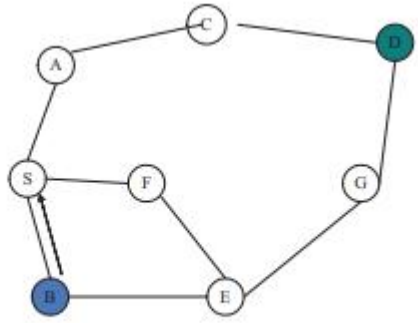
Node B is assumed to be a malicious node. When node B receives RREQ packets, it claims to have the routing to the destination node and sends the answer to the source node at the same time, using the routing AODV protocol. A response from the target node is also possible. Everything works well if the reply from a typical destination node reaches the RREQ source node first; however, if node B is closer to the source node, the reply from node B may reach the source node first. Furthermore, while delivering a false message, node B does not need to verify its RT since its answer is more likely to reach the source node first. As a result, the source node believes the routing discovery procedure is complete, disregards any other reply messages, and starts sending data packets. The forged route is now complete. As a consequence, node B consumes or loses all packets that pass through it. The black hole attack is named from the fact that Node B creates a black hole in the network.

Authentication Mechanism (Figure 1)

We suggest an authentication method for detecting black hole nodes in this section, which may be abused by hostile nodes. Without assuming the presence of any authentication infrastructure , which is generally not feasible in MANETs, to solve the aforementioned issues As shown below, an authentication method is built using the hash function, MAC, and P RF concepts. The source node examines RREP messages to decide which data packets should be allowed to flow via our suggested authentication method in this paper .Figure 1 Discloses The Black Hole Attack.



(a) Network Flooding of RREQ



(b) Propagation of RREP Message

Figure 1: Black Hole Attack

2. DISCUSSION:

We explain our simulation environment and provide the simulation results in this part.In order to create our simulation environment, we used the network simulator NS-2 [8]. To mimic the MAC layer, we utilize the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs and set the traffic source to Continuous Bit Rate (CBR). At a rate of four packets per second, CBR traffic is produced. For simulation purposes, a flat network is built and a variety of parameters are monitored. In the simulation, 50 mobile nodes move over a rectangle flat area. The simulation takes 1200 seconds to complete. In a rectangular area (1000 1000m2), the random waypoint model is chosen as a mobility model, with node speeds evenly ranging from 0 to 20m/s. Each node in the network is expected to have a 64-packet buffer and operate on a FIFO interface queue. To identify the black hole attack, we add the function of our approach to AODV.

NS-2 MAC layer protocol IEEE802.11 Mobility model Parameter Value Simulator Waypoints at random

Placement of nodes Unpredictable and consistent

1000 m2 – 1000 m2 of terrain

250s of transmission range

The AODV routing protocol was investigated.

2Mbps channel bandwidth

20 m/s maximum speed

CBR for application traffic

1200s simulation time

Mode of propagation There is a lot of empty space.

512-byte packet size

The total number of mobile nodes is 50.

Maximum number of connections: 20

The following metrics are used to assess our approach for preventing the black hole attack in MANETs.

- Control Overhead: To detect the black hole attack, the overhead of routing control packets is added. Because the objective is to compare data transfer to routing-related transmissions, transmissions are tallied rather than packets.

- The standard AODV is utilized as a benchmark against which the detection technique is measured. As can be seen, the control overhead does not vary much over time and does not exhibit a clear pattern when the maximum movement speed or simulation duration varies. False Negative Probability: We investigate and quantify the likelihood that the source node will fail to identify the black hole assault. The network's result of false negative probability is given in Figure 1. The detection probability rises as the node simulation duration increases, as seen in Figure1.

- Detection Time: This is the time it takes to detect a network that has been attacked by a black hole. It's calculated by subtracting the assault detection time from the traffic commencement time.

- Ratio of Data Package Delivery: This is the proportion of data packages delivered to the destination that are actually received. The data packet delivery ratio as a function of the number of black hole nodes[9]. The 2500 packets with rates are sent in the surroundings of 10 black hole nodes, as illustrated in Figure 5. As a consequence of eliminating black hole nodes, our approach maintains a reasonably high data packet delivery ratio.

TABLE I

SIMULATION PARAMETER

Parameter	Value
Simulator	NS-2
MAC layer protocol	IEEE802.11
Mobility model	Random waypoint
Node placement	Random, uniform
Terrain range	$1000 * 1000m^2$
Transmission range	250s
Examined routing protocol	AODV
Channel bandwidth	2Mbps
Maximum speed	20m/s
Application traffic	CBR
Simulation time	1200s
Propagation mode	Free space
Packet size	512 bytes
Number of mobile nodes	50
Maximum connection	20

3. CONCLUSION:

We examined the routing security problems of MANETs in this article, detailed the black hole attack that may be conducted against a MANET, and suggested a viable solution based on the AODV protocol to avoid the black hole attack while simultaneously protecting the network from additional hostile activity. An authentication method replaces the requirement for a public key infrastructure (PKI) or other types of authentication infrastructure, which are often impractical in MANETs. It will be explained how to manage infinite message authentication by switching one-way-hash chains and how to prevent a malicious node from forging a reply if any node's hash key is ultimately revealed to all nodes. Even in static networks, mobile nodes have the freedom to leave, thus node mobility will be addressed in the future[10].

REFERENCE:

[1] Y. F. Yuan, "Black hole binaries in the universe," *Scientia Sinica: Physica, Mechanica et Astronomica*. 2017.

[2] D. Bak, M. Gutperle, and R. A. Janik, "Janus black holes," *J. High Energy Phys.*, 2011.

[3] R. Emparan, P. Figueras, and M. Martínez, "Bumpy black holes," *J. High Energy Phys.*, 2014.

[4] G. Ruppeiner, "Thermodynamic black holes," *Entropy*, 2018.

[5] A. B. Nielsen, "Black holes and black hole thermodynamics without event horizons," *Gen. Relativ. Gravit.*, 2009.

[6] Wang Ding-xiong, "Can black-hole entropy be quantized ?," *Chinese Astron. Astrophys.*, 1991.

[7] K. A. Kabe, "Black Hole Dynamic Potentials," *J. Astrophys. Astron.*, 2012.

[8] N. Dadhich, J. M. Pons, and K. Prabhu, "On the static Lovelock black holes," *Gen. Relativ. Gravit.*, 2013.

[9] X. Calmet and R. Casadio, "What is the final state of a black hole merger?," *Mod. Phys. Lett. A*, 2018.

[10] I. D. Soares, "A boosted Kerr black hole solution and the structure of a general astrophysical black hole," *Gen. Relativ. Gravit.*, 2017.