In Mobile Adhoc Networks, Detecting and Overcoming Black Hole Attacks

Arvind Kumar Pandey, Assistant Professor

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

Email Id- dr. arvind.p@arkajainuniversity.ac.in

ABSTRACT: A mobile Adhoc Network (MANET) is a collection of self-contained mobile nodes that dynamically create a multi-hop radio network without the need of any pre-existing infrastructure. Infrastructure. Because of its unique features, such as a scarcity of resources, MANET's topology is constantly changing, and there is no centralized management. Is vulnerable to network layer assaults of many kinds. On-Demand Ad hoc The Autonomous Overlapping Distance Vector (AODV) is a self-starting distance vector. a routing protocol for MANETs whose security has been jeopardized by"BlackHole" attacks are a specific kind of assault. This rogue node promotes itself as having the most direct route to the destination. Destination during the route finding process, causing the procedure to be disrupted Network performance is degraded and actual communication is lost. We install the base node in the network in the suggested manner. Improves the likelihood of many malicious nodes being detected in the network and network

KEYWORDS: AdHoc Network, distance vector, Routing Protocols, AODV, Black hole Attack.

1. INTRODUCTION:

The Mobile Adhoc Network (MANET) is a self-configuring multi-hop radio network in which each node serves as both a source and a router, assisting each other in passing data that isn't intended for them. It is helpful in many real-life scenarios from military to civilian, such as search and rescue operations, data gathering, combat fields, and virtual classrooms and conferences , because to its fast and low-cost deployment with minimal infrastructure requirements. Mobile phones, laptops, PDAs, and other devices that have limited computing, communication, and energy resources make up MANET nodes[1]. MANET is more susceptible to assaults than wired networks due to key distinguishing characteristics such as open medium, limited energy, dynamic changing topology, no centralized supervision, no tight border, and wireless connections.

In today's world of communication, security is paramount. The majority of routing protocols is built on the premise that all network users are trustworthy and would cooperate. However, if countermeasures are not included into the system's early design, the network's fundamental function, communication, may be endangered at all levels, particularly at the network layer[2]. Proactive, reactive, and hybrid protocols are the three main types of routing protocols. Proactive is a table-driven protocol that refreshes routing information on a regular basis. DSDV and WRP are two examples. Reactive protocols are on-demand protocols, which mean that routes are only changed when the source requests it. AODV and DSR are two examples. Hybrid is a mix of reactive and proactive methods. ZRP and TORA are two examples.

This paper examines the Black hole Attack, one of the most serious attacks on the network layer in Adhoc networks, and proposes a behavioral strategy to mitigate its effects[3]. The remainder of the paper is organized as follows: Section II discusses the AODV protocol in MANET, while Section III discusses the Black hole Attack in AODV. Section IV also includes a short overview of the literature on black hole attack prevention and detection. Our suggested technique for detecting and isolating malicious nodes from the network is described in Section V. The suggested technique's simulation results and performance assessment are presented in Section VI, and the method is ultimately evaluated in Section VII. Section VII concludes with a discussion on the future scope of effort[4].

Adhoc Distance Vector Protocol on Demand (Aodv)

Every node in an Adhoc network has a routing table with information on how to go to a certain destination. When a node in an AODV network needs to interact with another node that isn't immediately in its range, it looks for a route in the routing table. If an entry cannot be identified, the node initiates a route discovery procedure and broadcasts a route request message (RREQ) throughout the network. The node that receives the request looks in their database for the destination node route. If a new route is discovered, the Route Reply Packet (RREP) is uncast to the source; otherwise, if an outdated route or no route is found, the request is rebroadcast in the network. After receiving the RREP, the source begins transmitting data packets. Link breaks are common as a result of random node migration[5].

When a node detects a connection failure, it sends a Route Error (RERR) message to the relevant precursor list of the IEEE 225 routing table, which eliminates any entries with compromised routes. A Black hole Attack is a kind of Dos attack that may be carried out by a single node or a number of nodes .These may be either internal or external network nodes[6].

The black hole attack takes use of the AODV routing protocol's characteristics to fabricate RREQ and RREP packets by lowering the hop count and raising the Destination sequence number, falsely claiming the best path to the destination. It swallows all packets delivered to it without passing them on, resulting in a network black hole. is an illustration of what I'm talking about. Node 'B' is behaving in a malicious manner. When node "S" wishes to transmit data to node "D," it broadcasts an RREQ packet across the network. It is received by Nodes ‘1', ‘2', and ‘B'[7].

Because Node ‘B' is malicious, it does not check its routing database for the route and uncast RREP packet to source. Node ‘S' receives a response from node ‘B' first, considers it the shortest route, and begins transmitting data to ‘B'. Instead of sending data packets, the malicious node drops them, degrading network performance. AODV, despite its high packet arrival rate, is vulnerable to a black hole attack because a malicious node may impersonate the hop count and destination sequence number during the route discovery phase, gaining access to the route and eavesdropping or deleting all packets as they come.

Many researchers have been interested in MANET security during the last decade. Many techniques have been suggested to defend networks against one of the most dangerous types of attacks known as Black hole. Every technique has its own set of advantages and disadvantages, as well as a defense against Black hole attacks. Some of the contributions have been organized by year in this section.[8]

Source node extracts information about next hop node from RREP packet and sends further route request (FRREQ) to next hop node, according to. The path for communication is chosen based on the response received from the next hop node regarding the RREP generator. In the first solution, the source node waits for responses from two or more nodes. In the second solution, the source node waits for responses from two or more nodes. It takes the entire route from the reply packet and checks for shared hops, then chooses the safe path based on that.

The disadvantage of this method is that data packets will never be sent if a shared hop cannot be identified. In the second method, each node in the network keeps two tables to keep track of the sequence numbers it sends and receives. The legitimacy of the response is verified based on the values. Latha proposed a method to reduce the likelihood of an attack in a network in which a node maintains a collect route reply table storing RREPs until the timeout occurs, and the next hop node in the table path is selected for communication based on the repeated next hop node in the table path.

Santoshi developed a method in which the status of the network is expressed using three parameters. Based on these three value thresholds, the number of sent out RREQ, received RREP, and DSN (calculated in each time slot) is computed to determine if the node is malicious or not. If a node gets an RREQ from a non-trusted node, Jieying e suggested encrypting the RREQ ACK REQ with the source's public key and sending it to the source. The source node decrypts it before encrypting it again using the receiver's public key and sending it back. Node is deemed authentic if the recipient gets the identical message that was delivered. Otherwise, RREQ will be disregarded.

A technique in which IDS nodes are placed in the network and monitor all nodes within its range. Its purpose is to calculate a node's suspicious value based on the anomalous discrepancy between RREQ and RREP sent by the node**.**

2. DISCUSSION:

The suggested approach takes use of the fact that black hole nodes broadcast route replies to every route request they get, regardless of whether they have a route to their destination. In this study, a Base Node (BN) is installed in the network to provide a method for detecting suspicious node activity. Once the node is determined to be malicious, BN sends out a block message to all nodes in the network, instructing them to cooperate isolate the node from all network communication. The identification of the base node and the identity of the black hole node are two fields in the block message produced by the base node.

When a block message is received, the normal node extracts the ID of the black hole node and adds it to the blacklist. Malicious node 5 is identified by base node 0, as shown in table 1. We assumed that in MANET, authentication exists and that only the base node may broadcast a list of black hole nodes.

The following is the method for detecting a black hole assault by a base node (BN):

BN sends a fake RREQ packet into the network at regular intervals, with the destination set to a randomly generated network address that does not exist in the network. It starts a timer after submitting the request and waits for responses from other nodes. When the timeout runs out, it looks for responses from nodes.

Because the fake RREQ is for nodes that do not exist in the network, genuine nodes do not respond. Only malicious nodes will respond since they do not verify their database for the path to destination before generating RREP. The BN node keeps track of all the nodes that have responded and generates a block message that is delivered to all nodes in the network. After receiving this block message from the base node, the other nodes add the identification of the black hole node to their block table and isolate it from further communication[9].

This technique significantly lowers the likelihood of a black hole assault in a network and aids in the detection of many black hole nodes in a network at the same time. Furthermore, nodes do not do any processing in order to identify rogue nodes. The amount of energy used and the amount of time it takes to complete a task are both decreased.

In the AODV protocol, NS2-2.34 is used to verify the detection and isolation of black hole attacks. To assess the effect of a black hole attack on a network, the following metrics are used: I throughput (ii) average end-to-end latency (iii) packet delivery ratio. For a normal network, a network with a black hole assault, and a network circumventing a black hole, these metrics are computed using AWK scripts.

The existence of a black hole node in a network lowers the PDR, as seen in the graph. In the presence of a malicious node, the suggested approach improves PDR. The amount of nodes and connections in the network has an impact on PDR. PDR is reduced as the number of connections increases[10].

Network throughput, which is the average rate of successfully delivered messages across a communication connection. The network's performance drops dramatically when a black hole node is present.hat in a regular network, there is a small increase in latency when compared to a network with a black hole, owing to the black hole’s rapid response since they do not examine the routing table for routes. The emergence of an event horizon—a barrier in space-time through which matter and light may only flow inward towards the black hole's mass—is a distinguishing characteristic of a black hole. Inside the event horizon, nothing, not even light, can escape. Because information from an event that happens inside the event horizon cannot reach an outside observer, it is difficult to establish whether such an event happened.

The existence of a mass deforms space-time in such a manner that particle trajectories bend towards the mass, as predicted by general relativity. This distortion gets so severe near a black hole's event horizon that no pathways leading away from the black hole exist. Clocks near a black hole seem to tick more slowly than clocks farther away from the black hole to a distant observer. An object falling towards a black hole seems to slow down as it approaches the event horizon, requiring an endless amount of time to reach their due to this phenomenon, known as gravitational time dilation. At the same time, all processes on this object slow down, making any light produced by the object seem redder and dimmer from the perspective of a stationary outside observer, a phenomenon known as gravitational redshirt.

The falling item eventually fades away until it is no longer visible. This process often occurs extremely quickly, with an item vanishing from vision in less than a second. Indestructible observers plunging into a black hole, on the other hand, are unaffected by any of these consequences when they pass the event horizon. They cross the event horizon after a limited period, according to their own clocks, which seem to tick regularly; in classical general relativity, owing to Einstein's equivalence principle, it is impossible to identify the position of the event horizon from local observations. The event horizon of non-spinning (static) black holes is perfectly spherical, while the event horizon of revolving black holes is oblate.

Singularity

A gravitational singularity, a region where the space-time curvature becomes infinite, may exist in the core of a black hole, as described by general relativity. This area assumes the shape of a single point in a non-spinning black hole, and it is spread out to create a ring singularity in the plane of rotation in a revolving black hole. The single area has zero volume in both instances. It's also possible to demonstrate that the single area includes all of the black hole solution's mass. As a result, the single area may be considered to have infinite density.

Observers falling into a Schwarzschild black hole (i.e., one that is non-rotating and uncharged) will be transported into the singularity once they pass the event horizon. They may extend the experience by speeding up to delay their fall, but only to a certain point. They are crushed to infinite density as they approach the singularity, and their mass is added to the black hole's entire mass. They will have been ripped apart by the increasing tidal pressures before that occurs, a process known as spaghettification or the "noodle effect."

It is feasible to escape the singularity in the case of a charged (Reissner–Nordström) or spinning (Kerr) black hole. Extending these answers as far as they can go shows the potential possibility of escaping the black hole via a wormhole into a new space-time. Traveling to another universe, on the other hand, is just a theoretical possibility since any disturbance would negate it. Around the Kerr singularity, it also seems to be conceivable to follow closed time like curves (returning to one's own past), which leads to causality issues such as the grandfather paradox. None of these strange phenomena are anticipated to withstand a thorough quantum treatment of spinning and charged black holes. The emergence of singularities in general relativity is often seen as a sign that the theory is breaking down.

However, owing to the very high density and therefore particle interactions, this breakdown is anticipated; it happens in a setting where quantum effects should explain these activities. Although there have been efforts to construct a quantum gravity theory, it has not been feasible to integrate quantum and gravitational phenomena into a single theory to far. It is widely assumed that such a theory would be devoid of singularities.

Sphere of photons

The photon sphere is a zero-thickness spherical barrier in which photons traveling along tangents to the sphere are imprisoned in a circular orbit around the black hole. The photon sphere has a radius 1.5 times the Schwarzschild radius for non-rotating black holes. Their orbits would be dynamically unstable, so any tiny disturbance, such as a particle of infilling matter, would create an instability that would increase over time, either allowing the photon to escape the black hole or spiraling deeper, ultimately crossing the event horizon. While light may still escape from the photon sphere, any light traveling in the other direction will be caught by the black hole. As a result, any light emitted by things between the photon sphere and the event horizon that reaches an outside observer must have been emitted by objects between the photon sphere and the event horizon. The radius of the photon sphere for a Kerr black hole is determined by the spin parameter as well as the specifics of the photon orbit, which may be protrude (the photon spins in the same direction as the black hole spin) or retrograde (the photon rotates in the opposite direction).

3. CONCLUSION:

This approach aids in the detection of black hole attacks in networks using bogus RREQ, and the results have been analyzed using PDR, throughput, and delay metrics. Future work can be extended by deploying more than one base node in the network, so that even if one base node fails, the network continues to detect black holes, and the network can be further analyzed using metrics such as Jitter. While the majority of the energy released during gravitational collapse is dissipated rapidly, an outside observer does not witness the process come to a conclusion. Due to gravitational time dilation, even though the collapse takes a limited amount of time from the perspective of infilling matter, a distant observer would witness the infilling matter slow and come to a stop just beyond the event horizon. The light emitted just before the event horizon forms takes an infinite amount of time to reach the observer, while the light emitted just before the event horizon forms takes an unlimited amount of time to reach the observer. As a result, the external viewer never sees the event horizon develop; instead, the collapsing material seems to fade and red-shift, ultimately fading away.

REFERENCES:

[1] Z. Xu, X. Hou, and J. Wang, "Possibility of identifying matter around rotating black hole with black hole shadow," *J. Cosmol. Astropart. Phys.*, 2018.

[2] J. van Dongen and S. de Haro, "On black hole complementarity," *Stud. Hist. Philos. Sci. Part B - Stud. Hist. Philos. Mod. Phys.*, 2004.

[3] H. C. Kim, J. W. Lee, and J. Lee, "Black hole as an information eraser," *Mod. Phys. Lett. A*, 2010.

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

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

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

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

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

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

[10] J. Armas, T. Harmark, and N. A. Obers, "Extremal black hole horizons," *J. High Energy Phys.*, 2018.