Mamet's Cooperative Black Hole Attack Prevention

Dr. Arun Kumar Marandi, Assistant Professor

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

Email Id- dr.arun@arkajainuniversity.ac.in

ABSTRACT: ***A mobile ad hoc network (MANET) is a self-contained network made up of mobile nodes that communicate via wireless links. In the absence of a fixed infrastructure, nodes must work together to provide the network functionality that is required. The AODV (Ad hoc On Demand Distance Vector) protocol is one of the most common routing protocols used in ad hoc networks. The AODV protocol's security is jeopardized by a type of attack known as a "Black Hole" attack. A malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept in this type of attack. To reduce the likelihood, it is suggested that you wait and check the responses from all of your neighbors to find a safe route. To combat the Black Hole Attack, we'll use a 'Fidelity Table,' in which each participating node will be assigned a fidelity level that acts as a measure of that node's reliability. If a node's level falls to 0, it is considered a malicious node, known as a "Black hole," and it is removed. In the presence of Black holes, computer simulations using GLOMOSIM show that our protocol provides better security and also better performance in terms of packet delivery than the traditional AODV, with minimal additional delay and overhead.***

KEYWORDS: ***Ad hoc Networks, Routing Protocols, AODV, Black Hole Attack, fidelity level.***

1. INTRODUCTION:

Infrastructure-based networks and infrastructure-less networks are the two types of wireless networks. Fixed base stations, which are responsible for coordinating communication between mobile hosts, are used in infrastructure-based networks (nodes). Ad hoc networks belong to the infrastructure-less network category, in which mobile nodes communicate with one another without the use of any fixed infrastructure[1]. An ad hoc network is a collection of nodes that are connected without the use of a predefined infrastructure. As a result, the functioning of ad-hoc networks is reliant on node trust and cooperation. Nodes assist one another in communicating network topology information and share network management responsibilities. As a result, in addition to acting as hosts, each mobile node also serves as a message router and relay for other mobile nodes.

Routing and network management are two of the most important networking operations. Depending on the routing topology, routing protocols can be classified as proactive, reactive, or hybrid. Tables are commonly used in proactive protocols. Destination Sequence Distance Vector is an example of this type (DSDV). On the other hand, reactive or source-initiated on-demand protocols do not update the routing information on a regular basis. It is only propagated to the nodes when it is required. Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector are two examples of this type (AODV). Hybrid protocols combine reactive and proactive strategies. Zone Routing Protocol is an example of this kind (ZRP). In all types of communication networks, security is a significant issue, but ad hoc networks confront the biggest difficulty owing to their intrinsic reliance on other nodes for transmission. As a consequence, an Ad hoc network may be subjected to a wide range of assaults[2].

The AODV Routing Protocols (A. AODV Routing Protocols) are a set of protocols

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is a dynamic link adaption of the DSDV protocol. . A routing table is kept by each node in an Ad-hoc network, which includes information on the path to a certain destination[3].

The node broadcasts the RREQ (Route Request) packet from the 2008 ACADEMY PUBLISHER. Every node that gets an RREQ packet first checks to see whether it is the packet's destination, and if it is, it responds with an RREP (Route Reply) packet. Whether it is not the destination, it consults its routing database to see if it has a route to the desired location. If it doesn't, it broadcasts the RREQ packet to its neighbors. If it has an entry for the destination in its routing table, the next step is to compare the 'Destination Sequence' number in its routing table to the one in the RREQ packet. The sequence number of the last packet transmitted from the destination to the source is the Destination Sequence number. If the

routing table's destination sequence number is less than or equal to the one included in the RREQ packet, the node forwards the request to its neighbors. If the number in the routing table is greater than the number in the packet, the route is considered a 'new route,' and packets may be routed via it. After then, the intermediary node transmits an RREP packet to the node that received the RREQ packet. Through the reverse route, the RREP packet is transmitted back to the source. After that, the source node changes its routing table and transmits its packet via this path. If any node detects a link failure during the operation, it sends an RERR (Route Error) message to all other nodes that utilize this connection to communicate with other nodes. Figure 1 shows how this works[4].

Because AODV lacks security measures, hostile nodes may carry out a variety of attacks simply by not following the AODV rules. Many attacks against AODV may be carried out by a malicious node M. This article improves the AODV routing protocol's routing security by removing the danger of "Black Hole" attacks.

A Black Hole attack is a kind of denial of service attack in which a malicious node attracts all packets by falsely claiming a new path to the target, then absorbs them without forwarding them.

The term "cooperative black hole" refers to the malevolent nodes acting in concert. Take, for example, the situation. The source node is S, while the destination node is D. The intermediate nodes are nodes 1 to 5. The cooperating Black holes are Nodes 4 (B1) and 5 (B2). When a source node wants to deliver a data packet to a destination, it first sends out an RREQ packet to its neighbors. The RREQ is also received by the malicious nodes in the network. Because Black Hole Nodes are known for being the first to react to any RREQ, they send out the RREP right away. As seen in Figure 2, the RREP from Black Hole B1 arrives to the source node far ahead of the other RREPs. The source now begins sending data packets after receiving the RREP from B1. Instead of sending data packets to their destination, B1 just dumps them, or B1 sends all of the data to B2. Instead of sending it to the target, B2 just dumps it.

As a result, data packets are lost and never arrive at their intended destination.

A lot of study has been concentrated on the problem of collaboration in MANET. Several relevant problems are briefly discussed in this article.

Researchers have suggested methods for locating and destroying a single black hole node. The case of multiple black hole nodes acting in concert, on the other hand, has not been addressed. When multiple black hole nodes are working together, for example, the first black hole node B1 refers to one of its teamma the source node S sends a “Further Request (FRq)” to B2 via a route other than B1 (S-3-B2).

Node S inquires of B2 as to whether it has a route to node B1 as well as a route to destination node D[5].

B2's "Further Reply (Frap)" will be "yes" to both questions because it is cooperating with B1. Assuming that the route S-B1-B2 is secure, node S now starts passing data packets, as per the solution proposed in.

However, in reality, node B1 consumes the packets, putting the network's security at risk.

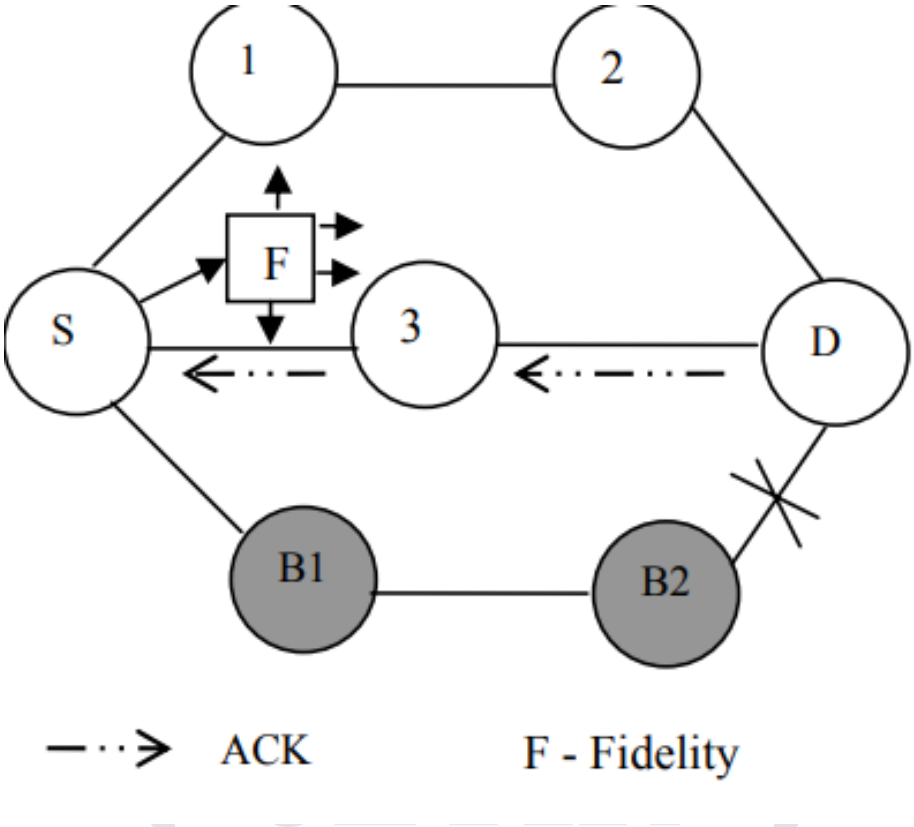

Figure 1: Receiving Acknowledgement and Broadcasting Fidelity Packets

2. DISCUSSION:

2.1. Application:

The CONFIDANT protocol is presented by Buchegger and Le Boudec. In a similar way as a watchdog, each node monitors the activity of its next hop neighbors. The information is sent on to the reputation system, which changes the node's rating. The trust manager decides whether to provide or accept route information, accept a node as part of a route, and so on based on the rating. When a node detects that a neighbor is misbehaving, it sends an ALARM message to its buddies. If a node's rating is determined to be intolerable, the path manager is notified, and any routes including the intolerable node are deleted from the path cache. This does not solve the issue of partial packet loss. In, Michiardi and Molva suggest the CORE system and discuss many associated problems. Every node in this system calculates a reputation value for each neighbor based on observations gathered in the same manner as watchdog. Subjective reputation, indirect reputation, and functional reputation all have different reputation mechanisms. Subjective reputation is computed directly from neighbors' past and current observations, with the previous observations being given greater weight to reduce false detection. The knowledge gathered via contact and information sharing with other nodes utilizing only positive values is referred to as indirect reputation. The global reputation value associated with each node is known as functional reputation. The system protects against assaults like denial of service by preventing the propagation of bad ratings. The service supplied to the misbehaving node is stopped when a neighbor's reputation falls below a specified threshold. The model's operation and performance were not documented[5].

OCEAN is a resilient packet-forwarding system proposed by Banal and Baker. OCEAN, like earlier systems, is built on the observations of nodes. Unlike prior methods, no ratings are shared, and each node relies only on its own data, obviating the need for trust management. The rating is based on a counter that counts the positive and negative steps a node takes, and the node is put to a defective list based on a faulty threshold. A DSR node appends an avoid list to every produced RREQ and an RREP depending on this list in the route selection procedure. A second-chance method is included to offer nodes that were previously deemed unruly a second chance to function. According to OCEAN simulations, a system that depends only on first-hand observation performs almost as well, if not better, than a method that also uses second-hand data. OCEAN also fails to appropriately deal with problematic nodes. When AODV is the underlying protocol, Bracha Hod emphasizes different elements of cooperative enforcement and

dependability in his thesis. It also introduces a scalable protocol that combines a reputation system with AODV to handle reputation fading, second-chance, liar resilience, and load balancing[6].

The suggested approach creates several reputation attributes and misbehavior reactions that are more AODV-friendly. The AODV protocol's security is jeopardized by a kind of attack known as a "Black Hole" assault. A rogue node promotes itself as having the shortest route to the node whose packets it wishes to intercept in this attack. To minimize the likelihood, it is suggested that you wait and verify the responses from all of your neighbors to choose a safe path. To counteract the Black Hole Attack, a ‘Fidelity Table' will be used, in which each participating node will be given a fidelity level that serves as a gauge of that node's trustworthiness. If a node's level falls to 0, it is deemed a malicious node, often known as a "Black hole," and it is removed. In the presence of Black holes, computer simulations using GLOMOSIM demonstrate that our protocol offers greater security and also higher performance in terms of packet delivery than the traditional AODV, with little extra delay and overhead.

2.2. Working:

We present a method that is a modification of the fundamental AODV routing protocol that can prevent multiple black holes from acting in the same group. We propose a method for detecting several black holes collaborating with one another, as well as a solution for finding a safe path to escape a cooperative black hole assault. Our approach presumes that nodes have previously been authorized and are therefore able to communicate. The black hole assault is described assuming this scenario. To counteract the Black Hole Attack, we'll utilize a 'Fidelity Table,' in which each participating node will be given a fidelity level that serves as a gauge of that node's trustworthiness. If a node's level falls to 0, it is deemed a malicious node, often known as a "Black hole," and it is removed. The RREQ is broadcast by the source node to all of its neighbors. The source then collects the responses for ‘TIMER' seconds, RREP. The following criteria are used to choose a response: The fidelity level of the responding node, as well as the fidelity level of each of its following hops, is included in each received. If two or more routes seem to have the same fidelity level, choose the one with the fewest hops; otherwise, choose the one with the highest.The participating nodes' fidelity levels are updated based on their consistent participation in the network. The destination node will send an acknowledgment to the source after receiving the data packets, and the intermediate node's level will be increased. The intermediate node's level will be decremented if no acknowledgement is received. The responses are gathered in a table known as the Response table. Source address, destination address, hop count, next hop, lifespan, destination sequence number, and source and destination header address will all be fields in the entry. The responses will be gathered until the timer runs out[7].

The following technique is used to choose a legitimate route from among the collected answers. The fidelity levels of the participating nodes will be stored in a fidelity table. The basic idea is to choose a node with a high level of fidelity. The fidelity levels of the responding node and its following hop are first examined.

The node is considered reliable if the average of their levels is greater than the specified threshold. When several answers are received, the one with the greatest degree of fidelity is selected. In the event that two or more nodes seem to have the same fidelity levels, the one with the lowest hop count is selected[8].

After evaluating the fidelity levels, the source S selects the response RREP-3, as illustrated in Upon receiving the data packets, every destination node sends an acknowledgment to the source node. The source node may increase the fidelity level of the intermediary node after receiving the acknowledgment since it has shown to be trustworthy and secure. If the source node does not get an acknowledgment within a timer event, the source node will decrease the fidelity level of the intermediate node that responded, as well as the level of the node that was provided as the intermediate node's next hop, in order to identify the cooperative attack. A cooperative black hole eliminates the possibility of positive next hop information.

The fidelity tables are shared amongst the participating nodes on a regular basis. Receiving acknowledgment and broadcasting fidelity packets when a node's fidelity level drops to 0, it means it

hasn't faithfully forwarded data packets, resulting in a Black hole. The discovery of a black hole must be communicated to the network's other participants[9].

3. CONCLUSION:

The routing security problems of MANETs are addressed in this article. The black hole attack, which may be readily launched against the MANET, is presented, along with a viable solution based on the usage of fidelity tables and assigning fidelity levels to the participating nodes. In the context of a cooperative black hole attack, our system receives a higher proportion of packets than AODV. Using the Global Mobile Simulator, the solution is discovered to accomplish the necessary security with minimum latency and overhead. The focus of future research may be on methods to minimize network latency[10].

REFERENCE:

[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] I. D. Novikov, "Black holes," *Surveys in High Energy Physics*. 2003.

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

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

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