In MANETS, A Cluster-Based Technique for Detection and Prevention of Black-Hole Attacks

Akash Kumar Bhagat, Assistant Professor

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

Email Id- akash.b@arkajainuniversity.ac.in

ABSTRACT: One of the most active study topics in the field of mobile ad hoc network (MANET) is secure routing. Due to the unique network features of absence of central authority, fast node mobility, frequent topology changes, insecure operating environment, and limited resource availability, developing a reliable security protocol for ad hoc routing is a difficult job. MANETs are well-suited for emergency circumstances such as natural catastrophes or military applications because to their minimal setup and rapid deployment. As a result, data transmission between two nodes should always be secure. A mobile ad hoc network (MANET) black-hole attack is an offense that occurs when hostile nodes attract data packets by falsely advertising a new path to the target. A clustering direction in the AODV routing protocol has been proposed for the identification and mitigation of black-hole attacks in MANET. Every member of the unit will send a single ping to the cluster head in order to determine the unique difference between the quantities of data packets received and sent by each node. If the problem is detected; all nodes in the network will hide the infectious nodes. The system's performance was measured in terms of packet delivery ratio (PDR), end-to-end delay (ETD), and throughput. The ns2 simulator is used to record energy simulation conclusions.

KEYWORDS: Ad hoc networks, Routing protocols, Mobile computing, Routing, Security, Throughput

1. INTRODUCTION:

A MANET is made up of several mobile nodes linked by wireless connections, with each mobile node serving as both a host and a router to create and maintain a route. When a source node wants to send data packets to a destination node, the packets must pass via intermediary nodes. As a result, in MANET, fast node deployment is critical for establishing a route. In a MANET, routing protocols are divided into two types: proactive and reactive routing protocols, as well as hybrid (reactive/proactive) routing protocols[1].

Proactive Routing Protocols are table-driven protocols that keep track of all potential destination nodes in a table and exchange routing messages in a sequential manner to keep the routing table information current, suitable, and accurate. When transmission from one node to another is needed, the route is already known and may be utilized. These protocols include the Optimized Link State Routing Protocol (OLSR) and Distributed Sequenced Distance Vector (DSDV) protocols.

On the other hand, reactive protocols such as AODV and DSR are on-demand routing protocols that only use the route determination process when necessary. When a route is needed, some form of Route Discovery procedure is used; however, since these protocols rely on cooperation between two nodes for packet forwarding, a noxious node in the network may cause a routing attack, disrupting MANET's regular routing activities. As a result of MANET's decentralized and dynamic character, the network may be subjected to a variety of assaults that may cause the network to be partitioned or destroyed. In MANETs, there are usually two kinds of attacks: passive attacks and active attacks.

The intruder listens to the communication channel quietly without altering the data packets. In an active assault, however, the intruder has the ability to alter or delete the raw data[2]. MANETs are useful in emergency circumstances such as natural catastrophes, hospitals, battlefields, conferences, and military applications because to their minimum setup and fast stationing.

Data transfer between two nodes, however, requires security. Active assaults, such as black hole attacks, rushing attacks, and wormhole attacks, have a significant impact on network performance. A black hole attack is a unique kind of assault that is often seen in Reactive protocols. A black-hole node is a malicious node that

draws packets by falsely claiming to have the quickest and most recent path to the target, and then drops them. These Black Hole nodes may harm the network in a variety of ways, including: Behavior as a Source node by violating the Route Request packet. Behavior as a Destination node by fabricating the Route Reply packet.

When promoting Route Request packets, reduce the amount of hops.

If the number of packets received to the number of packets transmitted is less than a certain threshold, the destination node will start the detection procedure. If there is a substantial discrepancy between the number of packets received by a node and the number of packets sent by it, the node is labeled as malicious and isolated from the network. Surveillance has long been a hot subject in MANET research. Various security methods and routing protocols for the avoidance of single and cooperative black hole attacks in the network have been suggested in[3].

To identify and avoid selective black hole attacks, Mohanapriya and Krishnamurthi developed the Modified Dynamic Source Routing Protocol (MDSR) in. To rule out the number of data packets it delivers to the destination, the source node selects the first shortest route to the destination. For real data transfer, the source node chooses the second shortest route. After then, the packet count and relayed data are compared. If a sound difference, i.e. abnormality, is detected, a nearby IDS node broadcasts a message briefing all nodes, thereby obscuring all nodes from the network.

The Routing Security Scheme for Reputation Evaluation (RSSRE) is presented in. The reputation assessment structure is based on correlation between the nodes that must be rated. When there are hostile nodes in cardinal Ad Hoc networks, it provides a method to build up cluster member cooperation for sending data packets to achieve better routing. The authors of presented a checkpoint-based Multi-hop Acknowledgement Scheme for detecting selective forwarding attacks that may randomly choose intermediary nodes as checkpoint nodes, resulting in acknowledgements for each packet received.

Every packet received by an intermediate node must be acknowledged, and the method must account for overhead. Furthermore, the channel is considered to be flawless. Full proof method, check-up algorithm, and diagnostic algorithm are three security algorithms proposed by Gao and Chen . The complete proof method was used to generate proof, while the checkup algorithm was used to verify source route nodes, and the diagnostic algorithm was used to locate malicious nodes in the network. According to method , each node should contain a Black hole Identification Table (BIT) that includes source, target, current node ID, packet received count (PRC), and packet forwarded count (PFC). If the discrepancy between PRC and PFC is significant, the node is labeled malicious and disconnected from the network. Chavda and Nunavut presented a method to avoid black hole attacks at the expense of overhead in [19]. The source node advances to accept RREP packets from various nodes and compares RREP (RREP R1, RREP R2), which compares the destination hop count of two route replies and chooses the route reply with the highest destination hop count if the difference between the two hop counts is not symbolically significant. Wang et al. suggested an access foundation of collaboration between nodes to enhance MANET productivity and efficiency by organizing nodes on the basis of trust mechanisms in[4].

The following assumptions underpin our model:

- the physical properties of all nodes are comparable.
- A node in the cluster's center is chosen as the cluster head.
- The total amount of data packets dropped by all black-hole nodes will be exactly half of the total.
- By default, the antecedent nodes and the destination node are considered trustworthy nodes.

A description of the protocol

In the AODV protocol, the source node broadcasts an RREQ packet to determine the best route to the destination. The RREP will be sent back to the source node by the destination node with the route. The black-hole nodes, as shown in Fig. 1, will also participate in the Path Discovery process and will claim the shortest route to the destination. If the black-hole node is chosen as the route, data packets may be dropped as illustrated in Fig. 1. In order to defeat the black-hole assault, a new strategy is devised. The enlarged nodes are split into clusters in this method, with each cluster having a cluster head and the other nodes being referred to as cluster members. Each cluster's cluster head may be selected at random. Some checkpoints are placed across the network to ensure that the number of data packets received by nodes and the number of packets sent by nodes are equal. Transfers may take occur inside the cluster or from one cluster to another, depending on where the source and destination are situated. Figure 1 discloses the Steps for Implementation.[5]

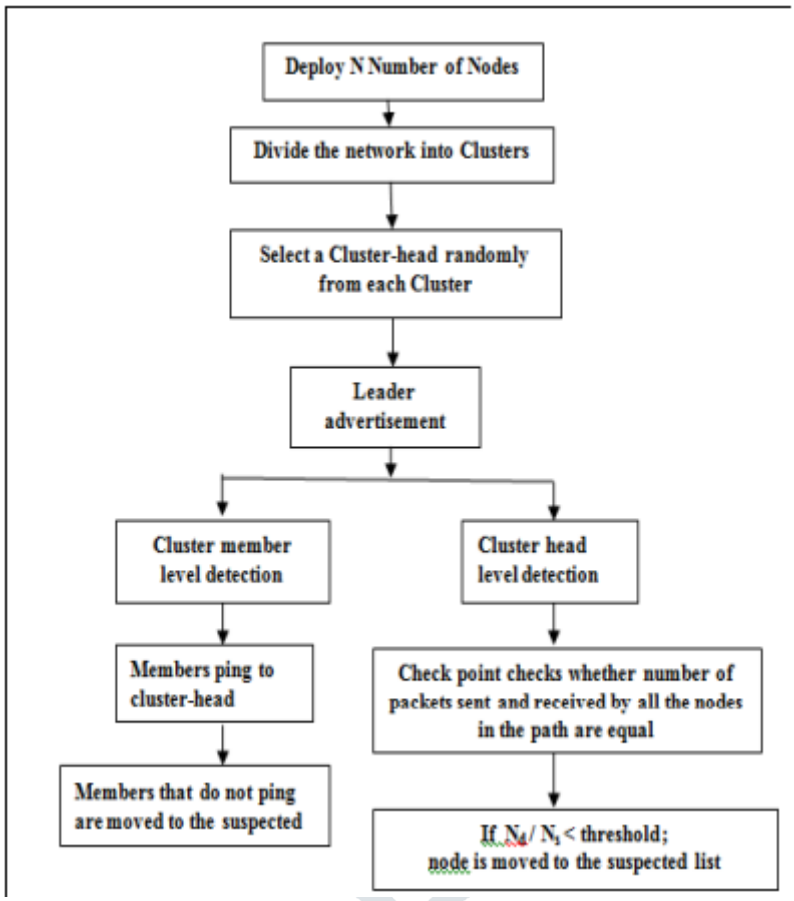

Figure 1: Steps for Implementation

2. DISCUSSION:

(a)Packet delivery ratio: PDelR changes solely with time in both instances. In the clustering method, the PDelR reaches 1 after 9 seconds, as seen in Fig 4. However, with the Modified AODV method, it becomes 1 after 23 seconds. The amount of data packets sent to and forwarded by the nodes in the route will be detected by mobile key points in the clustering method, and the data packet loss will be regulated[6].

(b)Throughput: is the number of data packets delivered per second. It may also be represented as bits per second. The simulation results of throughput are shown in Figure 6. The throughput achieved in our suggested method is almost three times that of the Modified DSR approach. At a time interval of 27 seconds, the Modified AODV method achieves a throughput of 1.5367 Kb/sec, whereas the clustering approach achieves a throughput of 4.8192[7].

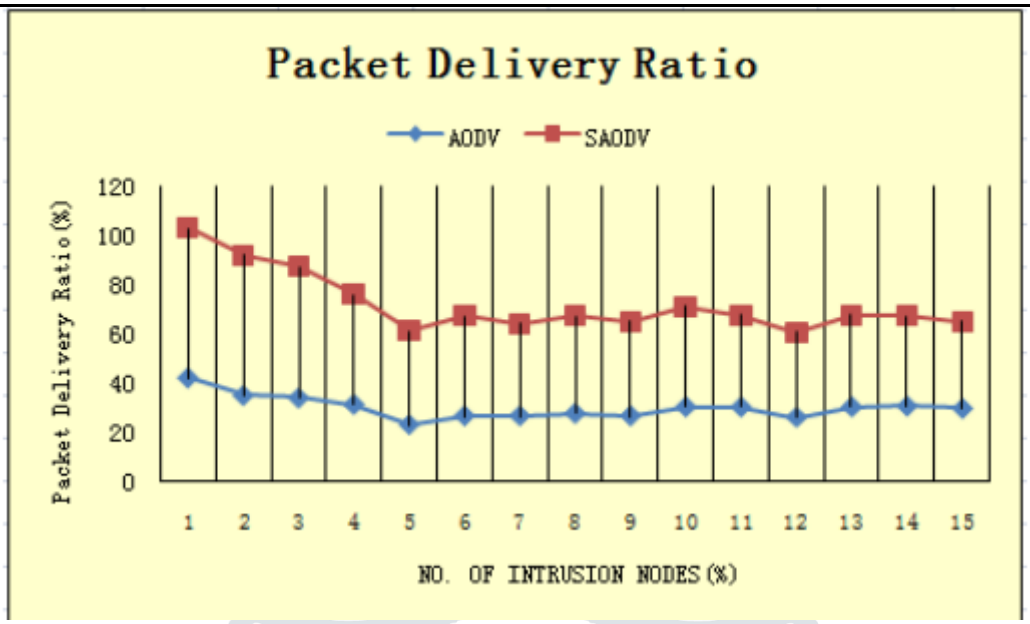

Figure 2: Packet Delivery Ratio

It is the ratio of the overall time difference across the total number of CBR packets transmitted and received to the time difference between each CBR packet sent and received[8]**.** Because many nodes in an ad hoc network fail due to a lack of energy, energy plays an important role. Simulations were used to look at the energy behavior of the various nodes. Assume that the number of data packets sent by the source to the destination is Ns, and that the data forwarding path is, Check-point (CP) maintains track of the amount of packets received by each node and passes them to the next level. When the source sends data packets to the destination node, check-point maintains track of how many packets the destination has received. Allow Ndnumber of packets to arrive at the destination. The chance of packets arriving to their destination is therefore as follows: Nd/Ns = Pd If Pd T, the check-point begins the process of determining whether or not the noxious node is present along the path. If it isn't, the destination sends a particular acknowledgement. The packet loss threshold is set to a value between 0 and 0.2. If packet loss exceeds 20% of total packets transmitted by the source node, the check-point initiates the black-hole identification procedure. After obtaining a good acknowledgment from the destination, the source node will send the following packet of data. Figure 2 discloses the Clustering in MANET[9].

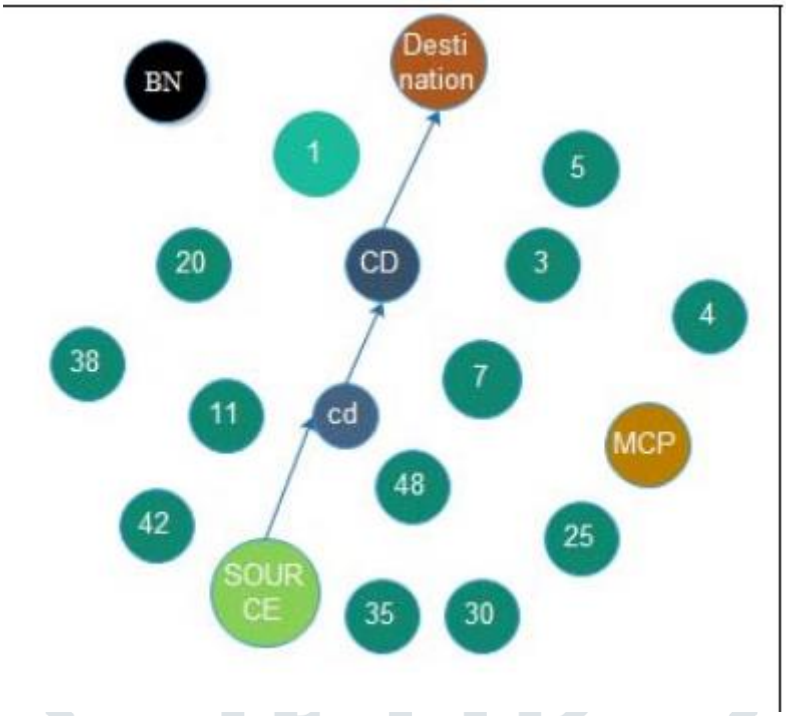

Figure 3: Clustering in MANET[10].

3. CONCLUSION:

The suggested lightweight method for detecting black-hole nodes in MANET is based on a simple affirmation mechanism. This method may be used with any demand routing protocol that is presently in use. In comparison to the Modified AODV method, it has been deduced that the suggested approach yields superior outcomes. In all methods, the Packet Delivery Ratio (PDelR) is 1, indicating that the system will result in complete packet delivery. The suggested method's Detection Rate (DR) is about three times that of the Modified AODV approach. Throughput is about three times higher in the clustering method than in the modified AODV approach. As a result, the suggested method has a greater data transfer rate. End-to-end latency and energy efficiency are also superior to the standard AODV protocol. Figure 3 discloses the Packet Delivery Ratio

Reference:

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

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

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

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

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

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

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

[8] M. Fähnle and G. Schütz, "Comment on magnonic black holes," *Journal of Magnetism and Magnetic Materials*. 2017.

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

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