IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at:

An efficient intrusion detection system on blackhole attack for Mobile Ad hoc Network

S. Nivetha
nivethacse555@gmail.com
Anna University BIT-Campus, Tiruchirappalli, Tamil Nadu

ABSTRACT

A Mobile Ad hoc Network (MANET), also known as wireless ad hoc network, is a self-configuration and infrastructure-less network of mobile devices connected wirelessly in a continuous manner. They are vulnerable to various kinds of attacks due to their dynamic nature and lack of a central control point. One of the most several network layer routing attacks in Blackhole attack. Among those routing attacks, black hole throws a challenge in interrupting and degrading the performance of data forwarding operation by dropping the data packets that are transferred through it. To ensure secure MANET an Intrusion Detection System (IDS) is being required. So in this research, we proposed an anomaly based IDS to detect black hole attack in MANET in turn computations have been performed using Neighbors Selective Acknowledgement. In the proposed method, all the nodes receiving data packet send an acknowledgment to the node from which it received it. If the source node receives an acknowledgment from a destination within the threshold time, the path is found to be protected against black hole node and originator takes no action. Otherwise, the source starts verifying nodes. Source node unicast verification message to all the nodes whose details it has stored. Our simulation experiment proves that detects black hole nodes efficiently with less false positive rate of detection and false positive rate.

Keywords— *Intrusion detection system, Black hole, AODV, Acknowledgment*

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are a collection of mobile nodes that inter-communicate on shared wireless channels. The topology of the network change with time due to the mobility of nodes. Nodes may also enter or leave the network. These nodes have routing capability which allows them to create multi-hop paths connecting node which are not within radio range. All the nodes of an ad hoc network depend on each another in forwarding a packet from source to its destination, due to the limited transmission range of each mobile node's wireless transmissions.

As nodes wish, they should be able to enter and leave the network. Multiple intermediate hops are generally needed to reach other nodes, due to the limited range of the nodes. Each and every node in an ad hoc network must be keen to forward packets for other nodes. Each node performs the role of both, a host and a router. Mobile Ad-hoc Networks (MANETs) characterized by irregularity of wireless links between the nodes, dynamic topology, and lack of secure boundaries, threats from compromised nodes inside the network, lack of centralized management, restricted power facilities, and Scalability.

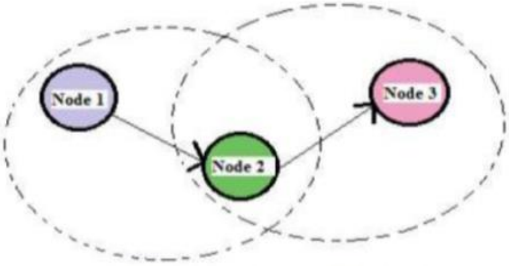


Fig.1: Mobile ad-hoc networks

Which networks that do not have any central controller or access point for communication is called the infrastructure-less networks. Mobile ad-hoc networks are self-configuring and infrastructure less in nature. With the help of wireless links, the different mobiles are connected with each other. The transformation of data from source to destination is done with the help of routing protocols. Routing protocols classify into three categories, Reactive, Proactive and Hybrid protocols. In Reactive Protocols, there is a route recognized from source to destination as per the need. The various reactive routing protocols are AODV (Ad-hoc On-Demand Distance Vector) etc. In proactive routing protocols route is predefined between the source and destination within a network. A routing table is maintained by each node which presents within the network.

1.1 Black hole attack

Figure 2 is an example of black hole attack in the mobile ad hoc networks. Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehaviour node who replies the RREQ packet sent from the source node and makes a false response that it has the quickest route to the destination node. Therefore node 1 incorrectly judges the route discovery process with completion and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node possibly drops or consume the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

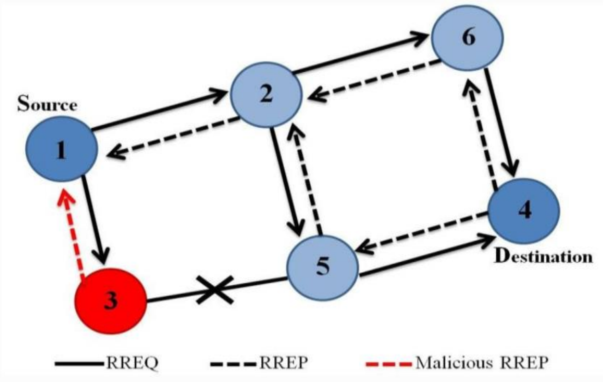


Fig. 2: Black hole attack

1.3 Routing protocols

The protocols may be categorized into two types, Proactive and Reactive. Another category of MANET routing protocols which is a combination of both proactive and reactive is referred to as Hybrid.

1.3.1 Ad-hoc On-Demand Distance Vector (AODV): The Ad-hoc On-Demand Distance Vector (AODV) is designed for use in infrastructure –fewer networks. AODV is a protocol the routes are shaped only when they are needed. It uses routing tables, one entry per destination, and sequence numbers to decide whether routing information is up - to - date and to prevent routing loops. An important feature of AODV is the protection of time - based states in each node: a routing - entry not recently used is expired.

2. RELATED WORK

Dilip Motwani et.al (2017) implemented a security mechanism is offered against a corresponding attack by multiple black hole nodes in a MANET. The reproduction approved out on the proposed scheme has produced results that establish the efficiency of the mechanism in the discovery of the attack as maintaining Constant Network Performance. The given simulation is developed using the proposed secure routing technique. When the proposed method is deployed network performance is improved and a large number of the packet is delivered to the destination. Communication happens between source node 9 and destination node 18. We calculate the performance of the old proposed method with attack and our new proposed method with attack The other proposed method which is reactive detection method eliminates the routing overhead problem from the on-demand way of route generation why network end to end delay, routing overhead are degrade sand packet delivery ratio, system throughput increases. But we have some limitations that are maybe resolved in future to removing security threats.

The simulation work is carried out by OPNET Modeler. To analyze the presentation of our proposed algorithm we use performance metrics ex. Network throughput, network load, packet send and received, packet dropped and end-to-end delay. Each cycle of the simulation runs for 20 minutes. The simulated network consists of 20 randomly allocated nodes in a space of 1000*1000 square-meters.In order to compare the performance of our proposed algorithm – three scenarios are created. In the first scenario, we have 20 reliable nodes without any blackhole node and prevented algorithm. .In the second scenario again we have 20 nodes but with one black hole node and no prevention algorithm. In the third scenario, we have the same 20 nodes with one black hole node and with our proposed algorithm. All scenarios are run under identical mobility and traffic conditions. The proposed solution can be applied to prevent single black hole nodes in a MANET .co-operative black hole attack cannot be prevented. The routing overhead also increases because of two extra control messages. There is a reduction in Packet Delivery Ratio and Throughput.

Packet Delivery Ratio (PDelR), Detection Rate (DR) and Throughput and simulation results are obtained using the ns2 simulator. Rate: Detection Rate is the total number of nodes detected (whether these are malicious or not) from the overall network, therefore the detection rate for the MANET should be as high as possible. In the proposed approach, the detection rate is about three times the Modified DSR approach. Throughput: is a number of data packets delivered per second. It is also expressed in a number of bits per second. Throughput obtained is near about three times that in Modified DSR approach. At the period of 27seconds; throughput for Modified DSR approach is 1.5367 Kb/sec and for clustering approach, it is 4.8192. Packet delivery ratio: PDelR in both cases differs only with time. Fig 4 shows that in the clustering approach at the period of 9 seconds, the PDelR becomes 1. But in Modified DSR approach, it becomes 1 at the period of 23 seconds, In case of MANETs, the Detection Rate should be as high as possible so as to detect a maximum number of nodes in the network whether these are malicious or not. Higher the value of DR, more secure is the network. In the clustering approach, Throughput is about three times the modified DSR approach. Thus the data transmission rate is higher.

The vulnerability of MANET is very high towards routing attacks such as blackhole, which drops all the packets instead of forwarding it to the destined node and results in data loss. This research paper focuses on analyzing the probable solutions pointed out by several eminent researchers to reduce the effects of blackhole attack in MANET. the network once they are in the range of it and may reduce the network performance by attacking it. The vulnerability of MANET is very high towards routing attacks such as Blackhole. Thereafter, the fact is that the AODV protocol is susceptible to the Blackhole attacks. Although research is still being carried out to modify the existing solutions for their viability in order to reduce the malicious effect of blackhole attack in the given network.

3. PROPOSED SYSTEM

In this project, we created a normal network with some normal (non-malicious) nodes and used plain AODV protocol for routing. Later we put some malicious nodes which are performing packet dropping attacks (Blackhole attacks). Let us consider Detecting black hole attack node when communication happens between the source and destination using selective acknowledgement method.

Let us consider the source node S sends out Packet 1 without any overhead except two bit of flag indicating the packet type. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an acknowledgement (ACK) packet to the source node S along with the reverse order of the same route. Within a predefined time period, if the source node S receives this acknowledgement (ACK) packet, then the packet transmission from node S to node D is successful. Otherwise, the Source does not receive the acknowledgement from Destination or Neighbour node within the given time period, then the Neighbour node is considered as a misbehaving node in the network. The concept of adopting a mixture system in Selective ACK greatly reduces the network overhead, but AACK still endure from the problem that they fail to detect misbehaving nodes with the presence of false misbehaviour report and fake acknowledgement packets.

3.1 Advantages

- Consumes Minimum Energy And Enhances Network Lifetime
- Identify malicious nodes efficiently through a false positive approach.
- Efficient routing technique

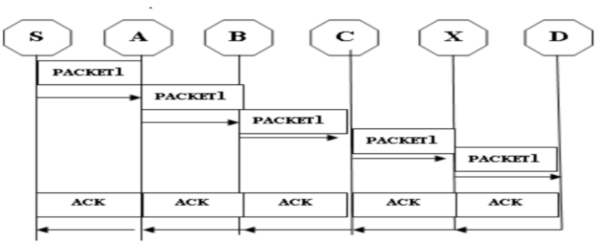
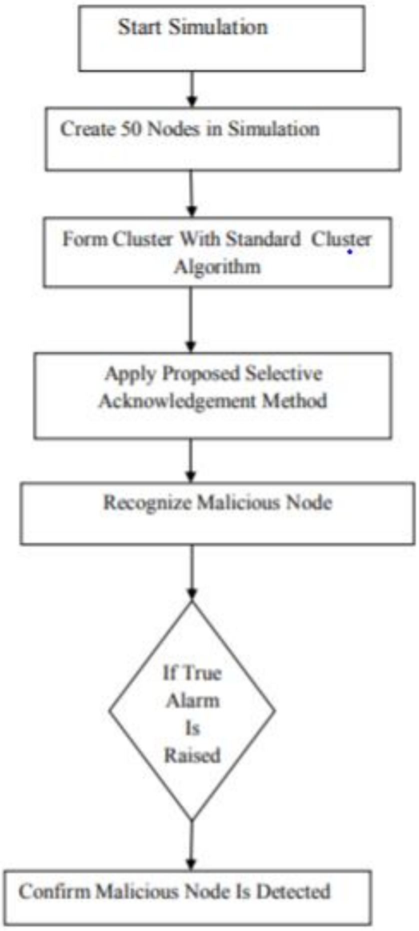


Fig. 3: ACK Scheme: the destination node is required to send acknowledgement packets to the source node

4. SYSTEM ARCHITECTURE


Start Simulation
Create 50 Nodes in Simulation
Form Cluster With Standard Cluster Algorithm
Apply Proposed Selective Acknowledgement Method
Recognize Malicious Node
If True Alarm Is Raised
Confirm Malicious Node Is Detected

4.1 Flowchart of the proposed scheme

4.1 Project steps

4.1.1 Route Request (RREQ): In this Source node (SN) is broadcast the RREQ in the network. If the RREQ entry exists in the Route Table (RT) then find the other RREQ in the network. If the entry does not exist in the RT than add a new entry in RT table. Here source node is also called an IDS node because we are using the Anomaly Based Ids System.

4.1.2. Route Reply (RREP): In RREP, the node sends the RREP to the RREQ node to have the highest DEST_SEQ (Destination Sequence) number for the fresh route to transfer the packet to the Destination Node (DN). If the CURRENT_TIME is less than TOTAL_TIME (CT <<<< TT) than it stores the DEST_SQ number in RREP Table. Otherwise, it selects the DEST_SEQ number from the RREP table. Selected DEST_SQ number is greater than the SRC_SQ number (Dest_sq >>>>> Src_sq) than it detects the malicious node and that malicious node id (M_ID) broadcast to all nodes and all node has store the M_ID in their RT table.

4.1.3. Detect the malicious node: The Detecting attacker node when communication happens between the source and destination using selective acknowledgement method. Let us consider three nodes A, B and C. If node A sends data to node B, then node B forwards the same data to node C. When Node C receives data sent by node A, it has to send back an acknowledgement to node B within the defined time period. Then node B sends the same acknowledgement to node A within the defined time period. If Node A receives the acknowledgement from node A within the given time period, then node B and C are considered as a genuine node in the network. If not node B and node C is detected as a malicious node.

4.1.4. Block Message: After Detecting the Malicious node, IDS node send the Block message to another node in the network. If malicious node id entry already exists in the RQ table than it Deletes all the entries from the RT table for malicious node. If not then add the malicious node into that list.

5. CONCLUSION

In this project, we detect the black hole and other attacks are also identified for efficient network performance. The existing system the detection mechanism for Blackhole nodes or any packet dropping node of that matter is basically done by observing the node for dropping of packets. The proposed system is IDS is detecting the malicious nodes on the basis of a number of packets dropped, if it finds any node dropping more packets it checks the energy level of that particular node. In future, to Improve False Positive Rate on Detecting Malicious node in MANET.

7. REFERENCES

[1] Kumar, Devendra, and Rupali Bhartiya. "An Implementation of Blackhole Detection and Prevention Method using AODV Routing Protocol in MANET Environment." International Journal of Computer Applications 150.9 (2016).

[2] Madhavi, SaniKommu. "An intrusion detection system in mobile ad-hoc networks." Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, 2008.

[3] Sharma, Romina, and Rajesh Shrivastava. "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network." International Journal of Computer Science and Network Security (IJCSNS) 14.3 (2014): 121.

[4] Rashmi, Ameeta Seehra. "Detection and prevention of black-hole attack in MANETS." International Journal of Computer Science Trends and Technology (IJCST)-Volume 2 (2014): 204-209.

[5] Su, Ming-Yang. "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems." Computer Communications 34.1 (2011): 107-117.

[6] Patel, Bhoomika, and Khushboo Trivedi. "Improving AODV Routing Protocol against Black Hole Attack based on MANET." IJCSIT) International Journal of Computer Science and Information Technologies 5.3 (2014): 3586-3589.

[7] Marti, Sergio, et al. "Mitigating routing misbehaviour in mobile ad hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[8] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual Southeast regional conference. ACM, 2004.

[9] Das, Rajib, Bipul Syam Purkayastha, and Prodipto Das. "Security measures for black hole attack in Manet: An approach." arXiv preprint arXiv:1206.3764 (2012).

[10] Patwardhan, Anand, et al. "Secure routing and intrusion detection in ad hoc networks." Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on. IEEE, 2005.