REVIEW ON ADAPTATIONS TO AODV ROUTING PROTOCOL TO MITIGATE BLACKHOLE ATTACKS IN MOBILE AD HOC NETWORKS

Muthaiah R, Kavitha T
School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT

Mobile ad hoc networks are self-organized, infrastructure-free network of mobile devices that are communicating through wireless. As they do not have a central authority, it is prone to many intrusion attacks. The compromised nodes may disseminate fake information to attract the traffic towards it. Blackhole refers the zone in a network where the network traffic is attracted towards the malicious node and dropped without informing the source. Blackhole is not obvious and that can only be found by observing the traffic. Ad hoc On Demand Distance Vector routing protocol is widely adopted for MANETs but it is vulnerable to blackhole attack. This paper involves the study of adaptations to the existing AODV protocol to prevent blackhole attack.

Key words: MANET, Blackhole attack, AODV, Packet drop attack.


1. INTRODUCTION

Mobile ad hoc networks (MANET) are wire free network which use to obtain routing possibilities through other nodes [1]. MANETs are widely used in personal area network, disaster relief efforts, commercial sector and military applications [2]. MANETs are self-forming and self-reconfiguring network. Each node in MANET has the freedom to move to any direction. Hence the network topology changes frequently. Each node must participate in forwarding the data that are intended to other nodes. This results in highly dynamic and autonomous topology. MANETs are dissimilar in architecture with respect to a wired network. Any host in a MANET may broadcast that it has the shortest path to the destination. Thus the traffic will be attracted to the host. If a node is compromised due to the blackhole attack, it may announce that it has the shortest path to the destination and it can attract the traffic. The captured data may be dropped without informing the source. Blackhole attack is a kind of denial-of-service attack [3]. The malicious node can also accomplish this attack in
Review on Adaptations to AODV Routing Protocol to Mitigate Blackhole Attacks in Mobile Ad hoc Networks

many ways. It may drop the selected packet for a particular destination node. It may drop every \( n \) packets for every \( t \) seconds. It may drop the packets randomly. The blackhole attack can be frequently deployed to attack MANETs, in which a node discards the packets instead of forwarding it. Blackhole attacks are of two types. Single blackhole attack comprises only of one malicious node. In collaborative blackhole attack more than one host will become malicious and mislead the other nodes in the network.

Due to the intuitive design drawbacks of routing protocol in MANETs, multiple researchers have conducted distinct experiments to propose different types of avoidance mechanisms and solutions for blackhole attack. Many techniques and detection schemes have been proposed to ensure the detection of blackhole attack at an early stage and to prevent the degradation of the network [4]. A routing protocol describes how nodes communicate to each other, publish information that allows them to choose paths between a source and destination. The routing protocol determines the efficiency of a MANET. Reactive routing protocol provides a route on request by flooding the Route Request (RREQ) packets. AODV is a broadly used on-demand routing protocol in MANET. AODV [5] permits the construction of paths to a destination and does not have need of the intermediate nodes to hold these routes for future use. It eliminates the count to infinity problem by utilizing the sequence numbers. The stale routes are discarded. Hence it reduces the number of active routes among the nodes. AODV identifies multiple routes between the source and destination. But a single route is chosen for communication. Routing table is kept for all routes including transient nodes. This protocol was designed to deploy in a network that has trusted nodes.

2. ADAPTATIONS TO AODV PROTOCOL TO OVERCOME BLACKHOLE ATTACK

The proposed work [6] involves comparison of sequence number of the source node and destination node. If the comparison resulted in a greater difference than the expected difference then it was concluded that the node as malicious and thereby removing the entry from the routing table. [7] is a preventive measure for the cooperative blackhole attack by modifying the AODV protocol. This scheme involved two main processes: 1. To maintain a table which consists of data routing information (DRI) 2. To check the reliability of the intermediate node. During route discovery each node sends two additional bits of information to the source node and a DRI table is maintained by each node. These additional bits carry information regarding the “from” and the “through” node. In the event of finding a secure route to the destination, the source node crosschecks the replies from the intermediate routes against the DRI table for the reliability of the intermediate nodes reply. If the intermediate node is present in the table then the source node maintains this as a secure path else it keeps looking for a reliable intermediate node and a secure route. The proposed method in [8] suggests to maintain a supplementary table (trust table) at each node which holds information about the reliable nodes including their address. A node will be added to the trust table of another node, if the broadcasting node’s behaviour is stable. Trust field is added to every RREP packet. The trust field can take any one of the three values (0 or 1 or 2). The trust field is initialized to 0. If the destination node is same as the node that replies then the field is set to 2. If the node that replies is in the trust table then the field is set to 1. By analysing the RREP packets received, the source node transmits if the field value is either 1 or 2 else it keeps waiting for a trust worthy route. The above modification provides secure routes but suffers network delay. The protocol [9] recommended a solution to enhance the performance of the AODV protocol. The RREP packet is provided with two parameters. One parameter maintains the information about the malicious nodes and the other parameter monitors the
update of the routing table. When the source node broadcasts the RREQ packet the malicious node will be the first one to send the RREP packet. This RREP is updated in the routing table if route update field is set to “true”. Later when another node send the RREP packet with a sequence number much less than the one updated in the routing table the entry is overwritten. This scheme helps to eliminate false route entry.

The architecture proposed in [10] includes multiple modules. Once the packet is received, it is classified as RREQ, Hello packet, etc, by the “packet classifier” module. An additional packet (ALARM) is added to the RREP packet. The content of every packet (except Hello) is extracted by the “extractor” module. A certain threshold is maintained. If the threshold is calculated accurately then it can prevent the network from malicious intrusion. Otherwise authenticated nodes are marked as blackhole nodes. The method to calculate the threshold determines the entire performance of the scheme. The algorithm proposed in [11], pre-process the RREP packets. Once the packet arrives, the sequence number of the packets are compared and if a packet has a very high sequence number, then it is assumed to be malicious and an ALERT message is broadcasted to other nodes. The malicious nodes are detached from the network. This algorithm suffers high network delay. In [12], an optimised algorithm for blackhole detection and prevention is provided. The sequence number of the node from which the transmission is to begin is stored in the routing table and the packet is forwarded to the intermediate node. After receiving the acknowledgement from the intermediate node its sequence number is updated. If the updated sequence number is found in the table then the transmission proceeds. On the other hand if the sequence number is not found, the node is said to be malicious. The algorithm suffers route acquisition delay. The suggested solution involves close monitoring of sequence numbers. Eventually the data packets must have higher rate than that of the contemporary packet identification number. The node in stable routing protocols getting along packet sequence number that it has approved and uses it to examine if the approved packet was instructed earlier from the uniform originating source. In this sequence, all nodes need to maintain two tables, to retrieve the lost data packet identification numbers. These tables are updated when the entire data packet arrives to the destination. The sender transmit the route request packet to its neighbouring nodes. Once this route request arrives at the destination, it will initiate a route reply to the source. This reply will contain the packet sequence number approved by the source node. This sequence number based mechanism provides a swift and stable path to get the acknowledgment. As the sequence number is included in the data packet itself, there will not be an overhead in the channel.

3. CONCLUSIONS

Blackhole attack is a severe security threat to a network. Many scholars have proposed various solutions and schemes to mitigate the blackhole attack. Most of the proposed solutions do not work for cooperative blackhole attack. When multiple nodes are compromised then there is no effective solution to mitigate blackhole attack. Blackhole attack affects and degrades the performance of a network. It also makes the network unreliable. When multiple hosts are compromised and mislead the other nodes in the network then the network cannot be used for any purposeful task. This becomes a grave danger when the network is employed for disaster relief. By gradually degrading the performance of the network and compromising the host nodes, a complete pack drop scenario is achieved in the network. Thus the network fails to serve its actual purpose. AODV is the mostly widely adopted protocol in MANET and as it suffers serious vulnerabilities many solutions have been put forward in order to improve the efficiency of the AODV routing protocol and thus preventing any form of malicious attack on the network. Blackhole attack imposes a very serious threat to the performance of AODV. AODV provides better scalability, robustness,
Review on Adaptations to AODV Routing Protocol to Mitigate Blackhole Attacks in Mobile Ad hoc Networks

reduced congestion and processing requirements. It eliminates the route table update for routes that are not used. Even after many proposed modifications to the existing protocol there is not any remarkable change in the performance of AODV against blackhole attack. AODV suffers high network delay. Though AODV provides many advantages over other routing protocols it also has its own downside. Latency, route discovery broadcast affect the performance of AODV to a greater extent. AODV has many commercial opportunities which involves home networking, range extension for cellular base stations, embedded computing applications, jungle telemetry etc. AODV is also used to enable computing where subnets do not exist. Enhancement of AODV is an active research area. Further works in near future are expected to reduce the latency and discrepancies of the existing AODV protocol and to find preventive mechanisms for cooperative blackhole attack.

REFERENCES


