International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 01,January-2015

Survey of Black Hole Attack Detection Techniques

Devanshu Matlawala, Jigar Mehta, Neha Mishra, Prof. Jignasha Dalal
Department of Computer Engineering, KJSIEIT
Ayurvihar Complex, Everard Nagar, Sion, Mumbai 400022
Maharashtra, India

***Abstract*— In wireless networking, a network which is set up temporarily with the help of mobile computers moving arbitrary in places that do not have a network infrastructure is called as an ad hoc network. Wireless ad hoc network is a decentralized type of wireless network. An ad hoc network typically refers to any set of networks where all the devices have equal status on a network and are free to associate with any other ad hoc network device in link range. In this type of network, the nodes communicate with each other by forwarding data packets. Therefore, the nodes find a path to the destination node using various routing protocols.**

However, due to various security vulnerabilities of the routing protocols, wireless ad hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. As the data packets in are not successfully reaching the destination node on account of this attack, data loss will occur. This paper presents the survey of latest black hole detection techniques that have been successfully implemented.

***Keywords*—AODV, DSR, DSDV, Black Hole, NS2**

I. INTRODUCTION

In Latin, ad hoc literally means "for this," meaning "for this special purpose" and also, by extension, improvised or impromptu. An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. Wireless ad-hoc networks are usually susceptible to different security threats and black hole attack is one of these. Black hole problem in MANETS is one of the serious security problems to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack. To support the connectivity nodes use routing protocols such as AODV (Ad-hoc On Demand Distance Vector) or DSR (Dynamic Source Routing). Ad hoc on-demand distance vector or AODV routing protocol is a reactive demand driven protocol which is the improved version of Distance Sequenced Distance Vector (DSDV) proactive table driven routing protocol. DSR is completely on-demand ad hoc network routing protocol collected of two parts: Route Discovery and Route Maintenance. This paper presents a survey of the latest implemented techniques that have been able to successfully detect the black hole problem and the malicious nodes from the wireless ad hoc network. This survey paper gives the advantages and the drawbacks of the methods and techniques that have been surveyed.

II. BACKGROUND AND MOTIVATION

Due to the extensive use of wireless ad hoc networks in daily applications worldwide, it is much necessary to pay attention to the growing security needs of the network and the of the participants of such a type of network. There are some techniques already implemented for detection of the malicious nodes from the network. But the main problem involved in doing so is that they need to overhear the entire network's communication which again creates a security issue and cannot be a reliable solution. Thus, a method to detect the attack of black hole in wireless ad hoc network without compromising the network's integrity or security has to be developed and with that in mind, this method has been proposed.

III. PROBLEM STATEMENT

In wireless ad hoc networks, due to less security and decentralized control over the nodal traffic, the networks are vulnerable to many security threats. Black Hole Attack is one of the common threats in which a malicious node attracts the nodes by advertising the shortest packet delivery path in the network and after getting the packets, it drops them from the network affecting the normal communication.

IV. REVIEW OF LITERATURE

The wireless ad hoc networks have been into practical use since long time and thus the problems and the security threats are well familiar with the users and the network designers. There is a decent study done on this topic and also a good amount of research and development has been done under this topic. The researchers have been keen on developing mechanisms to detect the attacks on the network and also been proposing methods to prevent the black hole attack.

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

A. *An Efficient Prevention of Black Hole Problem in AODV Protocol in MANET*

They proposed a method [1] which uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety, in other words, promiscuous mode means that if a node A within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A.

The following is a detailed process. Consider a scenario as shown in fig; node S needs to communicate to node D and node G is a malicious node. Node S floods a RREQ packet in the network and waits for the RREP packet to obtain a fresh route to the destination node D. Now, there are two possibilities; the RREP packet may be received either from the destination node itself or from an intermediate node. In case 1, when the RREP packet is received from the destination node itself, a route is established. In case 2, when the RREP packet is received from an intermediate node, a node preceding to the node which sent RREP packet switches on its promiscuous mode and sends a hello message to the destination node through this node. If the hello message is forwarded by this node to the destination, the node and hence the route is safe; otherwise, the node is a malicious node. In latter case, the preceding node floods an alarm message to the network about the malicious node to isolate it.

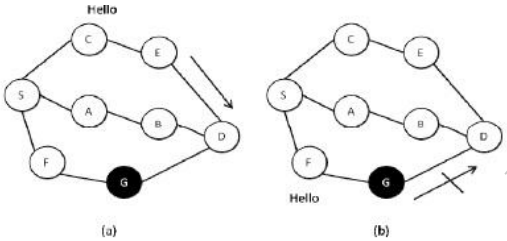

Fig. 1 Flow of Hello packet towards destination (a) a good node forwards it (b) black node does not forward it.

For example, (in Fig. 1) if node E sends a RREP packet, node C (the preceding node) switches on its promiscuous mode and sends a hello message to the node D through the node E. As node E is a good node, the message is forwarded by it. On the other hand, if node G sends a RREP packet, node F switches on its promiscuous mode and sends a hello message to the node D. As node G is a malicious node, it does not forward the massage. Now, node F floods an alarm in the network to isolate node G. It prompts node S to start a fresh route discovery process to the destination node D. The simulation results show that they are able to secure AODV protocol from black hole attack and achieve increased throughput while keeping the routing overhead minimal.

Advantage: There is a wide scope for detection of black hole attack and the detection of malicious nodes even if they aren't involved in the data packet transfer.

Drawback: As this method involves overhearing of the communication between nodes not directly involved in the transfer process, there are security issues and thus additional efforts are required to maintain secure data transfer.

B. *Detection and Eliminating Black Hole in AODV Routing*

In the start of the simulation, each node initializes black hole list and neighbour rating table[2] which includes neighbour address, packets sent to it and forwarded packets by them. While packet transfer takes place, it will check if the destination is the next hop neighbour. If it is not, promiscuous mode will be activated. Then the neighbour node will be monitored if it is forwarding the packets. Packets sent to field in the neighbour table are incremented as the data transmission goes on. Forwarded packets will be incremented or stay still according to the neighbour's action. Neighbour ratings[2] will be calculated when the timer goes off. If the ratio of forwarded packets and sent to packets is less than threshold, the neighbour node will be added to black hole list, routes through that node will be cleaned up and alert message will be sent to neighbours. Upon receiving an alert message, the node will check if the sender is in the black hole list and then update its black hole list. When a node meets a new neighbour node, it will ask its neighbours rating on the new one. By the time a reputation request is received, the sender will be checked whether it is a black hole and if it is not neighbour ratings will reset neighbour rating calculating time and calculate at once. Then the reply will be sent to the requested node.

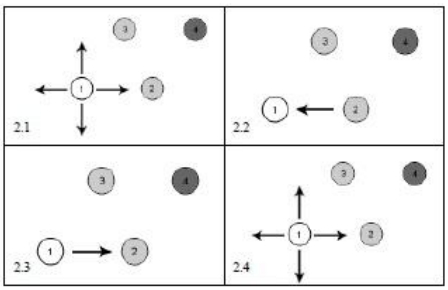

Fig.1Black hole detection

Node 1 wants to send data to node 4 but it does not have the route. RREQ packet will be sent to its neighbours by node 1 like in Fig 2. In this figure, node 2 replies the RREQ by sending RREP to node 1 that it has the route to node 4. Node 1 receives the reply and starts not only forwarding the data packets but also monitoring node 2's packet forwarding behaviour. Fig. 2 demonstrates node 1's actions. Node 1 keeps monitoring and it finds out that node 2 is dropping the packets, instead of forwarding them to the next hop node or send them to the destination. When node 1 is sure that node 2 is intentionally dropping the packets, it will add node 2 in the black hole list. Then route clean-up process will takes place and all the route entries to node 2 or through node 2 will be deleted from node 1's routing table. Finally, node 1 sends alert message to its neighbours informing node 2 is a black hole.

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

Advantage: Due to the presence of neighbour rating table, the Black Hole problem avoidance rate increases.

Drawback: This method involves much work overhead while dealing with the updates on the neighbour rating table.

C. Combat with Black Hole Attack in AODV routing protocol in MANET

In this paper, an approach has been proposed to combat black hole attack in AODV routing protocol[3]. In this approach any node uses number rules to inference about honesty of reply's sender. To participate in data transfer process, a node must demonstrate its honesty. Early of simulation, all nodes are able to transfer data; therefore they have enough time to show its truth (Though every node can be an effect less one). If a node is the first receiver of a RREP packet, it forwards packets to source and initiates judgment process on about replier. The judgment process is based on opinion of network's nodes about replier. The activities of a node are logged by its neighbours. These neighbours are requested to send their opinion about a node. When a node collects all opinions of neighbours, it decides if the replier is a malicious node. The decision is base on number rules[3]. The judgment is base on node's activity in network.

Rule1: If a node delivers many data packets to destinations, it is assumed as an honest node.
Rule2: If a node receives many packets but don't sent same data packets, it's possible that the current node is a misbehaviour node.
Rule3: When the rule2 is correct about a node, if the current node has sent number RREP packets; therefore surely the current node is misbehaviour.
Rule4: When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node.

Advantages: Faster detection of the malicious nodes as the communication goes through the set of rules. It avoids overhearing the network.

Drawback: There is no efficient detection of malicious nodes this method is based on neighbour's opinions and on node's honesty.

D. Performance Analysis and Prevention of Grey Hole and Black Hole Attack in MANET

The algorithm that is proposed in this paper is based on a course based scheme[4]. That is, a node does not observe every node in the neighbor, but only observes the next hop in current route path. For example, in Figure 1, S is the source node; D is the destination node; and P is a black hole. Node S is sending data packets to node D through the course S, P, Q, D. In this system, Node S only watches Node P, which is the next hop; but does not care Node 1 and Node 2.

If the overhear rate of next hop is less than threshold value (TH) then the node is considered as a Black Hole. After applying detection algorithm the performance of the network is further improved by applying dynamic threshold method. The node at which the attack is detected keeps the track of Black hole detection time. If Detection Time is less than expected Time then threshold values are updated. Due to dynamic threshold values the performance of network increases. Proposed algorithm isolates the black hole or gray hole node from path construction phase. To prevent Black hole node, the detecting node reroute the packet to another available path till no black hole or gray hole node is detected in path. DSR protocol sends the route Request for the packet and starts the route discovery process again.

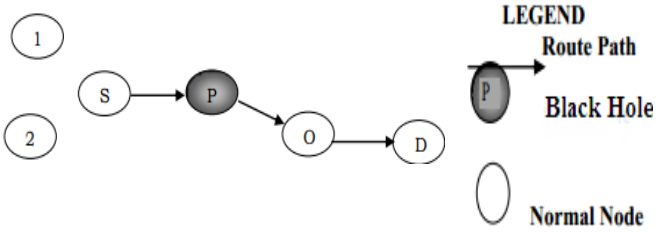

Fig. 3 Course Based Detection of Black Hole

Advantage: Each node is capable to detect the Black Hole attack individually without the need to overhear the whole network or dealing with the neighboring node's opinions.

Drawback: Sometimes, there are false alarms generated that lead to declaring a non malicious node as malicious.

V. PROPOSED METHOD

We have surveyed and studied all the above methods and have decided to implement and do some more work on the method mentioned in the last paper that is, Performance Analysis and Prevention of Grey Hole and Black Hole Attack in MANET because in the earlier methods there is a problem of overhearing of the entire network which is overcome in the last paper.

VI. CONCLUSION

In ad-hoc network, there is no strong networking infrastructure as it is just a temporary set up of nodes in order to establish connection amongst them for a limited period of time. The black hole attack is a common threat to the wireless ad-hoc networks where the malicious nodes enter the network and give out false responses the route requesting nodes in the network. These nodes then grab the packets and instead of passing them through, they drop the packets. This is a potential risk to the entire network as the packets do not get transferred and data loss occurs.

REFERENCES

1. Pramod Kumar Singh, Govind Sharma "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
2. HtooMaungNyo, PiboonlitViriyaphol "Detecting and Eliminating Black Hole in AODV Routing".
3. Mehdi Medadian, M. H. Yektaie, A.M Rahmani "Combat with Black Hole Attack in AODV routing protocol in MANET".
4. DeepaliRaut, KapilHande "Performance Analysis and Prevention of Gray Hole and Black Hole Attack in MANET."

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)