Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study of Blackhole Attacks, Their Detection and Prevention

Arunima Saini
Student CSE Department, Kurukshetra University
Kurukshetra, Haryana, India

Abstract- Today secure communication is the primary aspect while communicating in the networks. Internet has become the primary medium for communication which is used by number of different users across the network. Black hole attacks have become a major problem to wireless systems such as MANETs. MANET is a wireless ad-hoc network that allows collaboration in real time. Wireless ad- hoc networks are formed by a set of hosts that communicate with each other over a wireless channel. The Attacks on MANET interrupts network performance and reliability. Black hole attack also called as packet drop attack doesn't allow the passage of the packets forward in the network and hence restricting the services. Now my objective is to study the black hole attack, its detection and its prevention. Detection mechanism such as profile based detection, specification based detection and flow based detection are studied. Prevention techniques include algorithms such as AODVPlus, DBA-DSR scheme, reputation based scheme etc.

Keywords: – Blackhole attack, MANET, Misbehaving Nodes, AODV, DSR

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are the extension of the wireless networks [1] and are self configuring and infrastructure-less. A Fixed Infrastructure Wireless network provides communication among wireless nodes not directly through the Access Point (AP). The access points also works as a bridge. In the mobile ad hoc networks, the routing protocols play a major role in order to route the data from one mobile node to another mobile node. In such mobile networks, routing protocols are vulnerable to various kinds of security attacks such as blackhole node attacks.

The routing protocols of MANET are unprotected and hence resulted into the network with the malicious mobile nodes in the network. These malicious nodes in the network basically act as attackers in the network. One such attack on mobile ad hoc network is called blackhole attack. The mobile ad hoc network means MANET is nothing but the temporary network in which the mobile nodes collected independently on other mobile nodes in the same wireless network. The mobile nodes in these networks are moving arbitrarily all over the complete network. MANET networks are basically building temporary wireless networks and they are not requiring any kind of infrastructure for deploying as well as centralized administration. The communication among these mobile nodes depends on the kind of routing mechanism used called multihop routing protocols. These routing protocols are having the functionality of forwarding the data packets from sender mobile number to the intended recipient. Every mobile node in the mobile network is operating as the both forwarding node means routing operations and host node. Thus in other words we can say that, routing protocols for the mobile ad hoc network are introduced for building the communication routes as well as wireless communication network.

A. Characteristics

Mobile Ad hoc Network (MANET) is a collection of independent nodes that can communicate to each other and these nodes directly communicate with each other, where as intermediate node is needed to communicate two nodes which are not residing the radio range to route their packets [6]. Mobile adhoc networks are fully distributed and they do not need any infrastructure at any place so MANETs are robust and exile. Main characteristics of MANETs are:

1. Wireless communication done, nodes act as both hosts and routers.
2. No need of infrastructure and decentralized network.

B. Wireless Network Types

[1] An Infrastructure less Wireless Network does not have any fix infrastructure for the communication and routing. These kinds of networks don't have routers and the wireless nodes act like routers. These networks do not have any fixed topology.

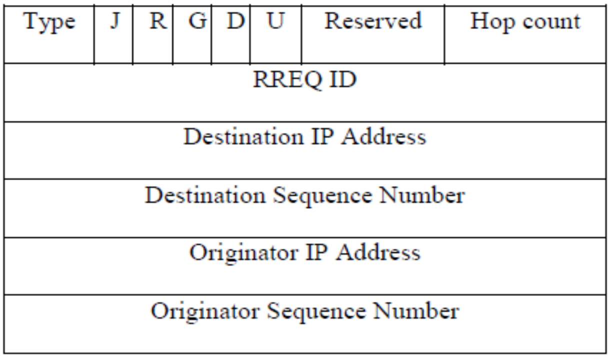
A mobile Ad hoc network consists of mobile nodes that use wireless transmission for communication. In MANETs the nodes can move from one place to another and the motion of the mobile nodes may be random or periodical. These networks do not have fixed infrastructure, fixed configuration and other controlling devices such as routers. The setup of these networks is very easy because these networks don't have a fixed infrastructure or a fixed topology and also they have a very less setup time. The routers are free to move anywhere in the network.

Mobile ad hoc networks (MANET) are widely used where there is little or no infrastructure available. A number of people with mobile devices may connect together to form a large group and even larger, later on they may split into smaller groups and so on. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack such as non availability, Denial of service attack, Fabrication attack etc.

C. The Routing Protocols

In recent years, several routing protocols have been proposed for mobile ad hoc networks and important among them are AODV, TORA etc. However, most of these MANET secure routing protocols did not provide a complete solution for all the attacks on MANET. They assume that any node participating in the MANET is not selfish and it will cooperate to support different network functionalities. ARAN – (Authenticated routing protocol) [2] is a solution which is a secure protocol and provides Integrity, Authenticity, Confidentiality, Non repudiation, Authorization and Anonymity. But an authenticated selfish node can cause interference to this protocol performance and can disturb the network by dropping packets.

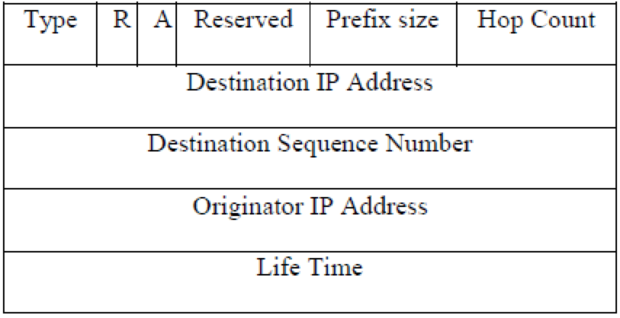
1) The AODV Protocol: AODV is a source initiated adhoc on-demand routing protocol in mobile network. Here, each mobile node maintains a routing table which maintains the next hop node information for a route to the destination node. Whenever a source node wants to route a packet to a destination node, it uses the specified route and if a fresh route to the destination node is available in its routing table. If the route is not available, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh route to the destination node specified in the RREQ packet or the destination node itself.



Type	J	R	G	D	U	Reserved	Hop count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

Fig. 1 RREQ Packet

Each intermediate node receiving the RREQ packet creates an entry in its routing table for the node that forwarded the RREQ message and the source node itself. The intermediate node or the destination node with a fresh route to the destination node, unicasts the Route Response (RREP) message to the neighboring node from which it received the RREQ packet. The intermediate node creates an entry for the neighboring node from which it received the RREP and then forwards the RREP in the reverse direction. On receiving the RREP packet, the source node updates its routing table with an entry for the destination node and the node from which it received the RREP packet. The source node then starts routing the data packet to the destination node through the neighboring node that first responded with an RREP.



Type	R	A	Reserved	Prefix size	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Life Time					

Fig. 2 RREP Packet

AODV like DSDV protocol is a dynamic protocol which is source initiated. Each node in these mobile networks maintains a routing table which contains information about the route to a destination. When a packet needs to be sent by a node, the node checks in the routing table to find whether a route to the destination is already available or not. If yes, then it uses that route to send the packets to the destination. If route is not available or if the previously entered route is inactive, then the node initiates a route discovery process. [8] An RREQ (Route REQuest) packet is broadcasted by that node. Every node that receives the RREQ packet first checks if it is the destination node for that packet and if yes then it sends back an RREP (Route Reply) packet. If the node is not the destination, then it checks in its routing table to determine if it has a route to the destination. If not then an RREQ packet is relayed by broadcasting it to its neighbors. If its routing table has an entry to the destination, then the comparison of the 'Destination Sequence' number to that of current sequence in the RREQ packet is performed. This Destination Sequence number is the sequence number of the last packet sent from the destination node to the source node. If the destination sequence number present in the routing table is less than or equal to the one contained in the RREQ packet, then the node relays the request packet further to its neighbor nodes. If the number is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. [8] This node then sends an RREP packet to the node through which it received the RREQ packet and the packet gets relayed back to the source node through the reverse route. After this, the source node updates its routing table and sends its packet through this reverse route. During this activity, if any node identifies a link failure then it sends an RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. Since AODV has no security mechanisms, therefore malicious nodes can perform several attacks just by not behaving according to the AODV rules.

<table>
<tr><td>Type</td><td>N</td><td>Reserved</td><td>Dest Count</td></tr>
<tr><td colspan="4">Unreachable Destination IP Address (1)</td></tr>
<tr><td colspan="4">Unreachable Destination Sequence Number (1)</td></tr>
<tr><td colspan="4">Additional Unreachable Destination IP Addresses (if needed)</td></tr>
<tr><td colspan="4">Additional Unreachable Destination Sequence Numbers (if needed)</td></tr>
</table>

Fig. 3 RERR Packet

2. DSR Protocol Dynamic Source Routing: It is a protocol developed for routing in mobile ad-hoc networks. It works as follows: Nodes send a ROUTE REQUEST message; nodes that receive this message put themselves into the source route and forward this message to their neighbors, unless they receive the same request before. If a receiving node has a route to the destination, it does not forward the request, and instead sends a REPLY message containing the full source route. It may send the reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible because of the asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it, and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out, this is an indication of a short path.

D. Blackhole Attack

In computer networking, a blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them.

[3] When the packets reach this malicious node, they merely disappear, as a matter of fact, they are said to have been disappeared into a blackhole in universe. In fact, the blackhole node impersonates the destination node by sending a spoofed route reply packet to the source node that have initiated the route discovery, hence deprive the packets from the source node. A blackhole node has two properties. First, the node takes advantage of the ad hoc routing protocol, such as AODV or DSR and advertises itself as having a valid route to the destination node. Second, the node consumes the intercepted packets. This type of attack is dangerous and may cause immense harm to the network.

In the following figure 4 imagine a blackhole node B1. When node 1 broadcasts RREQ packets to the nodes 2, 4, B1 receives it. Node B1 being a blackhole node, does not check with its routing table for the requested route to destination 5. And hence it immediately sends back an RREP packet, claiming a route to the destination node. Node 1 receives the RREP packet from B1 ahead of RREP from other nodes. Node 1 assumes that the route through node B is the shortest route and sends packets to the destination nodes through it. When the node 1 sends data to B it drops out all the data and behaves like a blackhole node.

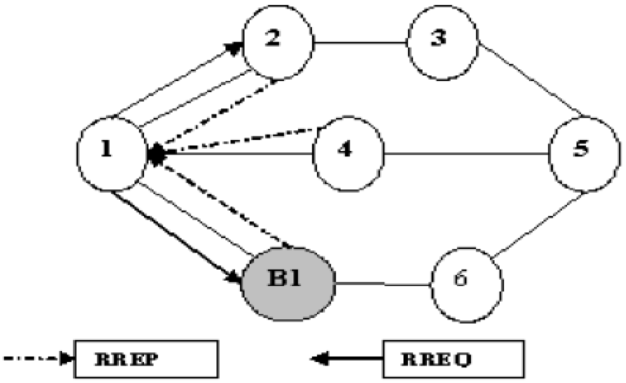


Fig. 4 Blackhole attack scenario

E. Misbehaving Nodes in MANET

Node misbehavior can be defined as any form of disobeying the protocol specification to obtain the given goal at the expense of honest participants. A node may misbehave in order to save its resources e.g. process time and energy. A misbehaving node continues to perform any type of misbehavior till it gain sufficient benefits [7]. Fig 5 shows the packet forwarding in a network with regular nodes and in the presence of misbehaving nodes. Misbehaving nodes can be usually classified as selfish nodes and malicious nodes. Selfish nodes are those nodes which misbehave to save their resources like power whereas malicious nodes disturb the network operations by their malicious activities. These misbehaving nodes may participate in the route discovery and route maintenance phases [5] and transmit control packets which can benefit it. However they refuse to forward data packets. Malicious nodes, on the other hand, will participate actively in both route discovery and maintenance phases and transmit the control packets since they need a path to send the data packets so that they can alter or drop those packets.

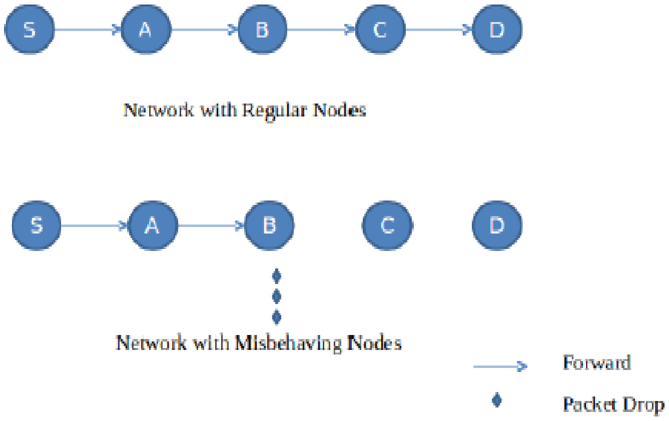


Fig. 5 Network with regular noded VS misbehaving node

II. LITERATURE REVIEW

Secure efficient algorithm for the detection of the blackhole attack. This algorithm firstly identifies the blackhole node in the given Mobile Ad hoc Network and then removes the entries for that node from the routing table. This algorithm is implemented in a popular reactive routing protocol, called AODV. The beauty of the algorithm is that it works in both the cases when there is no communication (i.e., a node is idle) and when a node is communicating (node is not idle).

ARAN, a reputation-based scheme to be combined with one of the secure routing MANET protocols to make it detect and defend against selfish nodes and their misbehavior has been explained and the problem associated with it is studied and a solution to overcome it. An explanation of the different phases of this scheme and analysis of the various forms of selfish attacks that this scheme defends against are studied. Temporal table is more efficient and more secure than ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.

DBA-DSR scheme, a feasible DSR-based solution to mitigate blackhole attacks in MANETs. Simulation results showed that (1) the original DSR heavily suffers from blackhole attack in terms of network throughput and packet delivery ratio, (2) the proposed DBADSR scheme performs better than the DSR scheme in terms of network throughput rate and minimum packet loss percentage. In future, we plan to extend the proposed DBA-DSR scheme so that it can handle the case of cooperative blackhole attacks in MANETs as well.

The reputation of the nodes can not only be used to increase the throughput of an ad hoc network, but also to motivate other nodes to cooperate. The reputation scheme improves the throughput to 65% with 40% malicious nodes, in a network where the nodes are static. The cost of this improvement is the increased number of route requests. The throughput can be improved at the expense of extra messages. This can be done by making the nodes exchange their reputation databases by using cryptographic protocols for ascertaining the credibility of the source of information and the correctness of the reputation information obtained. Quantitative models for calculating threshold values R will increase the usability of the proposed approach.

AODVPlus scheme that utilizes a mesh structure and alternate paths. This scheme can be incorporated into any ad hoc on-demand unicast routing protocol to improve reliable packet delivery in the face of node movements and route breaks. Mesh network generates multiple alternate routes without any extra overhead on the network. Alternate routes are utilized only when data packets cannot be delivered through the primary route. Unlike in earlier works where local route repairs were not considered as important [10] for performance comparison of ad-hoc routing protocols, its importance is highlighted in this work. To improve the AODV performance there is the need for fast locally corrective mechanisms which avoid the traditional route error broadcast to trigger fresh route discovery in the event of link failure and other congestion related situations. This paper has proposed improvements using a mechanism which provides robustness to mobility and local congestion control in AODV.

SCF+ scheme is used to solve problem of selfish replica allocation in MANETs. This procedure is based on the SCF technique [5]. The existing SCF technique may suffer from the poor system performance because it loses the original distance information between nodes when building the SCF tree. To cope with this limitation, we measure the degree of selfishness by considering both node distance and selfish behavior in an integrated manner. A novel node leveling technique is also proposed that utilizes the memory space of all connected nodes, including selfish nodes as well. In this strategy, nodes prefer to allocate replicas to near, nonselfish nodes, even though far away nodes are not necessarily selfish. One important consequence of this strategy is that risky and far-away nodes, which are likely to disconnect frequently, are efficiently measured.

Various types of misbehaving nodes found in the network and the reasons for their misbehavior. An overall idea about misbehaviors at two layers of the OSI model; i.e., the network layer and MAC layer and a brief description of various existing schemes to detect the misbehaving nodes and to reduce the effect caused by them in the network is discussed. The Reputation based schemes mostly based on overhearing technique have many drawbacks and led the way to active acknowledgement based schemes. The credit based schemes requires the source node to keep the amount of virtual money required for the transaction of the packet. These schemes impose a burden on the source node.

Table I. Summary of Authors and Techniques Used

Author	**Technique used**	**Advantage**	**Disadvantage/ Future work**
Neelam Khemariya and Ajay Khuntetha	Detection of single and cooperative blackholes	It detects the black hole nodes in case when the node is not idle and also detects the Blackhole nodes in case when a node is idle.	As the future work, this algorithm can be implemented for some other dangerous network layer attacks such as Grey hole or Wormhole attack etc.
R. Sudha and Dr. D. Sivakumar	ARAN	Reputation-based scheme to be combined with one of the secure routing MANET protocols, ARAN, to make it detect and defend against selfish nodes	Temporal scheme combined with ARAN provides more security
Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat	DBA-DSR scheme	DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput	Doesn't deal with cooperative blackhole attacks in MANETs
Prashant Dewan, Partha Dasgupta and Amiya Bhattacharya	Reputation scheme	The reputation scheme improves the throughput to 65% with 40% malicious nodes, in a network where the nodes are static.	Increased number of route requests
Abdul-Fatau Adam	AODVplus scheme that utilizes a mesh structure and alternate paths	The mesh network generates multiple alternate routes without any extra overhead	As part of future work, this scheme can be incorporated into other ad hoc on-demand unicast routing protocol
V. Giri Babu and T. Sreenivasulu	SCF+ procedure	Novel node levelling technique that utilizes the memory space of all connected nodes, including selfish nodes as well. Limitations of SCF has been removed	Plan to improve the current levelling technique by considering the frequency of disconnections

III. CONCLUSION

A blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. When the packets reach this malicious node, they merely disappear, as a matter of fact, they are said to have been disappeared into a blackhole in universe. In fact, the blackhole node impersonates the destination node by sending a spoofed route reply packet to the source node that have initiated the route discovery, hence deprive the packets from the source node. Blackhole attacks can slow down the network to great extent by dropping out the intended packets to be sent to the destination node. These attacks can be prevented using efficient techniques such as mesh network schemes; AODV based schemes etc and could be applied to a network ranging from few nodes to larger number of nodes.

REFERENCES

[1] Neelam Khemariya and Ajay Khuntetha, "*An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs"* International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013

[2] R. Sudha and Dr. D. Sivakumar, "*A Temporal table Authenticated Routing Protocol for Adhoc Networks"* 978-1-4577-1894- 6/11/$26.00©2011 IEEE

[3] Isaac Woungang, Sanjay Kumar Dhurandher, Rajender Dheeraj Peddi, and Mohammad S. Obaidat , "*Detecting Blackhole Attacks on DSR based Mobile Ad Hoc Networks"* 978-1-4673-1550-0/12/$31.00 ©2012 IEEE

[4] Prashant Dewan, Partha Dasgupta and Amiya Bhattacharya *On Using Reputations in Ad hoc Networks to Counter Malicious Nodes* Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS'04) 1521-9097/04 $ 20.00 IEEE

[5] Abdul-Fatau Adam , "*Performance enhancement of AODV over DSR on demand routing protocols - aspect of packet salvaging in ADOV"* 978-1-4244-6252-0/11/$26.00 ©2011 IEEE

[6] V. Giri Babu and T. Sreenivasulu, "*Detection of Selfish Node and Replica Allocation Over MANETs"* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 9, September 2013

[7] R. Gomathi, Sony Jose and J. Govindarajan, "*A Survey on Detection Schemes of Misbehaving Nodes in MANETs"* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 9, September 2013

[8] Latha Tamilselvan, Dr. V Sankaranarayanan, "*Prevention of Blackhole Attack in MANET"* The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 0-7695-2842-2/07 $25.00 © 2007