Middle-East Journal of Scientific Research 23 (5): 944-947, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.05.22220

ABRD: Acknowledgement Based Route Discovery and Detection of Black-Hole Attack in MANET

[1]Kareemullah Shaik and [2]Md. Ali Husaain

[1]KL University, Computer Science and Engineering, Vaddesewaram, India
[2]KL University, Electronics and Computers Engineering, Vaddesewaram, India

Abstract: Mobile Ad hoc Network (MANET) is a collection of many autonomous nodes, these nodes of MANET's acts as a node and router. These networks are also known as infra-structure less networks. In real time MANET's are being used in applications such as disaster relief, Military, emergency operations, vehicular communication, campus networks and so on. Because of open medium, limited bandwidth, dynamic topology, limited battery power and lack of central authority MANET's are very much vulnerable to various types of security attacks in network. Attackers attack MANET at different layers of its protocol stack. Due to inefficient routing protocol these attacks are more at Network layer since there is no efficient routing protocol. In this paper we study the effect of black-hole attack on AODV routing protocol. Also we propose a mechanism known as secure route discovery to discover valid and secure path between source and destination using acknowledgement based technique, this mechanism will easily detect malicious nodes and defend the black-hole attack in mantes.

Key words: MANET · Black-hole attacks · PDR · AODV

INTRODUCTION

Wireless ad hoc networks are special class of wireless networks. Under wireless ad hoc networks we are having Wireless Mesh Networks (WMA), Wireless sensor networks (WSN), Vehicular Ad-hoc Networks (VANET's) and Mobile ad-hoc networks (MANET's). All these networks are known as Self-Organizing networks. Since the node's doesn't have any central authority to monitor the network and to perform network operations. So it is the responsibility of nodes to find the optimal route and forward the data from source to destination. MANET's have many potential application areas such as Military battle fields, Disaster management, conferencing, campus networks, vehicle to vehicle and vehicle to roadside communication and many more.

In traditional networks i.e. Wired and wireless networks there are *routers* and *access points* to connect the nodes of a network. MANET's lack of these central authorities and nodes of network directly communicates with each other and forwards packets over themselves. Due to their intrinsic MANET's are very much vulnerable to various kinds of attacks. For Example packet replication, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, routing-table overflow and poisoning, et [1], sinkhole attacks, snooping attacks, worm-hole attacks, black- hole attacks [2]. Among these attacks black-hole attack is the major one which affects the routing and packet drop rate (PDR) in MANET's. There is lot of research going on to counter this attack.

In black-hole attack, a malicious node send false routing data, claiming that it has a optimal and shortest routing path and causes other good nodes to route all their data packets through it. This attack is mostly possible with the re-active routing protocols for example AODV.

There are many routing protocols in MANET's and they are categorized as proactive, reactive and hybrid. In reactive routing protocols AODV (Ad Hoc on Demand Vector) protocol [3], nodes of network find routes only when necessary. Whereas proactive routing protocols like OLSR (Optimized Link State Routing Protocol) [4], nodes in network obtain routes by periodic exchange of topology information.

Corresponding Author: Kareemullah Shaik, KL University, Computer Science and Engineering, Vaddesewaram, India.

Preliminaries

AODV Protocol Overview: AODV is a reactive routing protocol [3] that is popularly used in mobile ad hoc network. It maintains routes only between nodes which need to communicate. For example source node A wants to send packet to destination node E and it does not have fresh path between source and destination it starts route discovery by sending route request (RREQ) messages to its neighbors. The next neighbor sends the same to its next node until RREQ message reaches the destination. After receiving the first RREQ now the destination node sends a route reply (RREP) to the source node through the same path in which RREQ arrived at destination. The same RREQ received at destination are ignored by it. Routes discovery process of AODV is shown in Figure 1. In the figure A (source node) wants to send data to node E (destination node). Initially the source node A check the route map for communication. In case if it does not find a route to destination it starts broadcasting RREQ to the network. Node B, D, F receives the RREQ and renews the route to its previous hop and checks whether they have route to destination if so they send RREP to node A (source node). It also checks for duplicate RREQ and discard such messages if it has already received. In case node does not have a valid route it again broadcast the RREQ. The same process is performed until they reach the destination node E. When the node E receives RREQ its send the RREP to A and establishes the route for data transmission. If the source node receives the multiple RREP's then its selects the RREP with highest destination sequence number (Dst_Seq), it also checks for same Dst_Seq if it find the same selects the RREP whose hop count is smallest.

Route Error message should also be handled by the AODV, when there is a route disconnection in network it should be informed to the source node. In example if Node leaves the network then node F generates Route Error (RERR) messages and update list with invalidated address of node F, then sends it to the node A.

Black-Hole Problem: In black-hole problem a malicious node claims that it has a short route to destination by utilizing the routing protocol. It receives the packets from source node and intercept those packets without forwarding to destination node [5]. There are two basic types of black-hole attacks, they are Single black-hole attack and Collaborative attack.

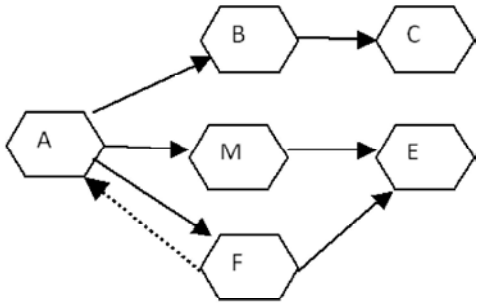

Fig. 1: Example MANET nodes sending messages.

Black-Hole Attack on AODV Protocol: There are different types of black-hole attacks as below

- Single Black-hole Attack,
- Cooperative Black-hole Attack

- Internal Black-hole Attacks and
- External Black-hole Attack.

Single Black-hole Attack: In this type of attacks there will be only one malicious node in network which tries to utilize the routing protocol and intercept the data packets without forwarding to the destination, Here Malicious node may is a node belonging to network (Insider) or may be from outside the network (outsider).There are so many mechanisms proposed to defend the single black-hole attacks both as insider and outsider but they are having some pitfalls.

Cooperative Black-hole Attack: Cooperative black-hole attacks means, there will be more than one malicious node in the network and tries to misuse the routing information and create a severe PDR loss in network. Here these malicious nodes may be insider or outsider of a network.

Internal Black-hole Attacks: This type of attack is caused by node of network which is misbehaving while different faces of routing protocol working. Here node will act as malicious during route discovery or during packet transfer. This type of attack is more vulnerable to detect and defend because of detecting internal misbehaving of nodes in network.

External Black-hole Attacks: External black-hole attacks is a attack performed by a node that is outside of network, which tries to use the routing protocol with false

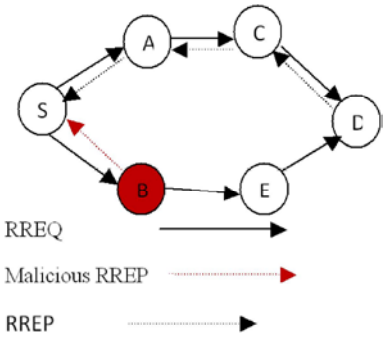

Fig. 2: Malicious node consuming packets

advertises (fake RREP) and claims that it has a fresh route to the destination. Detecting and identifying is challenge to researchers since the network poses the property of mobility where nodes joins and leaves network dynamically.

Problem Definition: In single black-hole attack there will be single malicious node which tries to utilize the routing protocol and consumes the data packets from source node without forwarding them to the destination. Due to this attack PDR reduces a lot. For example in Fig 2 Source node S wants to send data to destination node D through intermediate nodes A, B, C and E. S initiates route discovery process and broadcast RREQ to the network. If B is a malicious node then it will claim that it has shortest active route to destination node as soon as it receives RREQ packets. Then it will generate RREP and send the RREP to the source node before any other node. In this way source node will think that this s the active route and ends the route discovery by discarding other RREP's from other nodes which are having genuine active route to destination. Now source node starts sending data packets to the malicious node B which will consume the data packets without forwarding them to the destination node. This creates decrease in PDR (Packet Data Rate).

Related Work: Many schemes have been poposed to defend the black-hole attacks in MANET's like security aware ad ho routing (SAR) [6] uses the concept of trust level key authentication, Secure Efficient Ad hoc Distance Vector Routing protocol (SEAD) [7] uses hashing to authenticate the hop count and sequence number in DSDV protocol.Trusted Ad hoc On-Demand Distance Vector Routing (TAODV) [8] provides security using trust relationship in network. Ariadne [2] uses the shared key concept between ttwo node in DSR routing protocol.

Computational overhead is more in all the above schemes due to the management of keys, hashing and encryption decryption techniques in discovering the secure route between soure and destination. The other mechanism to provide security in MANET and to overcome the black-hole attack is Intrusion Detection System, but these techniques will increase the routing delay and routing overhead.

In addition various route discovery mechanisms are being proposed by research with the help of Swarn Intelligence (SI) [9], Hybrid approach using Ant Colony Optimization (ACO) enhanced by Multi agent System (MAS) [10]. But these provide computational overhead. Our mechanism is a light weight route discovery without any additional computations.

Our scheme discovers a secure route between source and destination without using any cryptographic techniques, hashing and trust level key authentications and also detect the black-hole nodes easily.

Proposed Algorithm: The main aim of the paper is to discover a secure route between source and destination in mobile ad hoc network while using AODV protocol at network layer. Since in AODV there is no exiting route between source and destination, it is the responsibility of protocol to discover route between source node and destination node. In the process of route discovery routing protocol is vulnerable to black-hole attack, where an adversary node claims to source node that it has a shortest route to the destination. Source node then start transmitting data packets to destination through the malicious node, but malicious node intercept and drop the packets without forwarding to destination. This affects the PDR (packet Drop Rate) of network. To overcome this type of attack we have proposed a new route discovery mechanism using acknowledgement. Acknowledgement Based Route Discovery (ABRD) working is as below.

Acknowledgement Based Route Discovery (ABRD): When a source node is intended to send some data to destination node, AODV protocol starts the route discovery mechanism. It starts transmitting RREQ to its neighbor nodes, neighbor nodes check whether they have valid route to destination or not, if so they send RREP and otherwise forward the RREQ to their neighbor nodes. At the same time when the route discovery is started in ABRD mechanism the neighbor node which receives the RREQ should generate an ACK packet which is shown in

Node ID	Int_node_count	Dest_flag

Fig. 3: Acknowledgement Packet

A	1	0

Fig. 4: Acknowledgement packet at node A.

D	3	1

Fig. 5: Acknowledgement packet at destination

Figure 1. The information in ACK packet is stored in DRDT table shown in Figure 2. The DRDT is dynamically updated until the RREP is generated at destination. We proposed two algorithms one for route discovery (Dynamic secure routing algorithm) and other for detecting malicious nodes.

Acknowledgement Packet (ACK Packet): An ACK packet is generated when a RREQ is received at intermediate nodes in network, by using the information in this packet DRDT is updated. The basic ACK packet is shown in figure 1 and example packet for ACK packet is shown in figure 2, In Acknowledgement packet there are 3 fields and they are

- *Node ID*
- *Int_node_count* - Intermediate node count
- *Dest_flag* - Destination flag

Node_ID: Node_Id is used to identify the nodes in network generally it may be the ip number of the node. At source node value is S in our scenario, when it reaches the intermediate node A its value is A and so on.

Int_node_count: While discovering the secure and dynamic route between source and destination we need to keep track of total number of node in between them and so we use intermediate node count to collect the nodes that form secure route from source to destination to transfer the data packets. By default the value of this field is 0. When it reaches the neighbor node of source then it is incremented by one. The same value is update in dynamic route discovery table.

Dest_Flag: Destination flag is used to judge whether the neighbor node which receives the RREQ is a destination or not. By default the value of this field id 0. When the neighbor node is a destination node then it is set to 1.

Dynamic Route Discovery Table (DRDT): DRD table is to find the dynamic secure route in between source and destination with an acknowledgement based scheme. It consist of following fields

- Src_node
- Dst_node
- Dest_seq
- Int_node_count

Src_node: The source node it use to change dynamically whenever RREQ reaches a neighbor node in network.

Dst_node: It Is destination node and it is fixed in the table target node id.

Dest_seq: Destination sequence number of AODV protocol, it is generated when RREQ is created and incremented by one when RREP is generated.

Int_node_count: This field is updated by fetching data from ACK_PACKET.

Table 1: DRDT format

Src_node
Dest_node
Dest_seq
Int_node_count

Table 2: DRDT at Source Node

At NOde	S
Src_node	S
Dest_node	D
Dest_seq	60
Int_node_count	0

Table 3: DRDT at intermediate node A

At NOde	S	A
Src_node	S	A
Dest_node	D	D
Dest_seq	60	60
Int_node_count	0	1

Table 4: DRDT at intermediate node B

At Node	S	A	B
Src_node	S	A	B
Dest_node	D	D	D
Dest_seq	60	60	60
Int_node_count	0	1	2

Table 5: DRDT at Destination D

At NOde	S	A	B	D
Src_node	S	A	B	C
Dest_node	D	D	D	D
Dest_seq	60	60	60	61
Int_node_count	0	1	2	2

Working of DRD Table: Dynamic route discovery table is used by all the nodes in a MANET to store the dynamic route discovered by the new proposed algorithm, in example scenario source node wants to send data to destination, so it broadcast the RREQ to its neighbors. Neighbors A and B receives the RREQ now the genuine nodes of MANET will send a acknowledgement to the source nodes as shown in Fig 4, DRD table is updated as in Table 3. Intermediate node count is recorded at every node and when the RREQ reaches Destination the destination sequence number is incremented and the int_node_count is not incremented. Source node checks the int_node_count when it is same for last two nodes it assumes that the RREQ reached the destination and accepts only that nodes destination sequence number as final and starts the data transmission through the intermediate node available in DRD table. Hence we can achieve secure data transmission without using any keys, cryptographic techniques in MANETS.

Algorithm: Dynamic Secure Routing.

- Source node broadcast RREQ to its neighbors
- Intermediate node receives the RREQ

If node is Destination
Set Dest_flag to 1 in ACK_PACKET and send it to source node
else
Increment the Int_node_count by 1 and
Send the ACK_PACKET to previous node from which it received the RREQ and
Re Broadcast the RREQ to the network neighbor nodes.
end if.

- Node receives ACK_PACKET then extracts the data and updates the DRD table

If node is source node
Update data and discard packet
else
Forward packet to the previous node.
endif.

- Repeat step 2 and 3 until Dest_flag is updated to 1.

If Dest_flag is 1.
Stop incrementing Int_node_count and send ACK_PACKET with same count.
End if.
Generate RREP

- At source node

If Int_node_count is same for last two nodes in route.
Send packets through this secure route.

In the Dynamic Secure Routing Algorithm a source node broadcast a RREQ message to its neighbor, the neighbor intermediate node receives the RREQ and checks whether the node is destination or not, if so then update ACK packet by setting dest_flag to 1 and send it to the source node. Otherwise increment the Int_node_count field in ACK packet and send it to the node from which it received the RREQ and re broadcast the RREQ to its neighbor nodes.

When a node receives an ACK packet then it reads the content and updates the DRD table, if the node is source node then it discards the packet. Otherwise if it is a intermediate node then it forwards the packet to its previous hop. Continue the same until the dest_flag is updated to 1, when the same becomes 1 then stop incrementing Int_node_count, send ACK packet according to same count and then generate RREP.

At the source node check for Int_node_count, if it is same for last two nodes then start data transmission through this secure route.

Algorithm to Identify Malicious Node:

- Source node sends RREQ to network
- If receiver node is Malicious node

It sends RREP with highest destination sequence number, no ACK_packet.
endif.

- Source node discards RREP without a ACK_PACKET from any node.

If no ACK_PACKET from node with RREP then
Node is Malicious.
Source node sets alarm with malicious node information to all other nodes.
end if.

In the detection algorithm firstly source node sends RREQ to network, when a malicious node receives this RREQ then it generates a RREP with highest destination sequence number as usually, but it does not send any ACK packet. At source node use to discard RREPs without ACK packet from any node in network, hence the source node declares the node as malicious and set the alarm with malicious node information to all other nodes in network.

CONCLUSION

Security is the key feature in MANET, due to its vulnerabilities MANET's are being attacked at different layer's, these attacks are more at network layer. The most dangerous attack is black-hole attack which decreases the Packet Drop Rate (PDR) in MANET. So we analyzed the working of major Ad hoc routing protocol AODV, the effect of black-hole attack on AODV protocol. Our mechanism proposes how to discover a secure route in between source and destination to transfer the data and also to detect the black-hole nodes in network causing packet drop rate (PDR). We proposed two algorithms one for discovering a secure route between source and destination and the other for detecting the malicious nodes in the network and sets the alarm to all the remaining nodes in network when a black-hole node is detected. We make use a of an additional packet known as ACK packet and an additional routing table known as DRD table to discover the secure route. Since there is a reliable route between source and destination the data can be transferred securely in between source and destination.

REFERENCES

1. Umang, S., B.V.R. Reddy and M.N. Hoda, 2010. Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications 5(17): 2084-2094. doi: 10.1049/ietcom.2009.0616
2. Yih-Chun, Adrian Perrig and David B. Johnson, "Ariadne: Asecure On-Demand Routing Protocol for Ad Hoc Networks", sparrow.ece. cmu. edu/~adrian/ projects/securerouting/ ariadne.pdf, 2002.
3. Perkins, C., E. Belding-Royer and S. Das, 2003. "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
4. Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2 and Yoshiaki Nemoto1 "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, 5(3): 338-346, Nov. 2007
5. Al-Shurman, M., S.M. Yoo and S. Park, Black-hole attack in mobile ad hoc networks. 2004:ACM.
6. Shilpa, S.G., N.R. Mrs, Sunitha and B.B. Amberker, " A Trust Model for Secure and QoS Routing in Manets", International Journal of Innovative Technology & Creative Engineering (Issn:2045-8711) 1(5): 22-31.
7. Yih-Chun Hu and David B. Johnson, v "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks" ELSEVIER Ad Hoc Networks 1 (2003) 175-192, doi:10.1016/S1570-8705(03)00019-2.
8. Xiaoqi Li, Michael R. Lyu and Jiangchuan Liu "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks" Aerospace conference 2004. Proceedings 2004 IEEE (ISSN: 1095323X) vol 2 6-13 march 2004, pp: 1286-1295.
9. Sharad Sharma, Sharad Sharma, Brahmjit Singh, "Hybrid Intelligent Routing in Wireless Mesh Networks: Soft Computing Based Approaches" I.J. Intelligent Systems and Applications, 2014, Vol 01, pp: 45-57. DOI: 10.5815/ijisa.2014.01.06
10. Vignesh Ramamoorthy, H. and Dr. D. Suganya Devi "A New Proposal for Route Finding in Mobile AdHoc Networks", I.J.Computer Network and Information Security, 2013, 7: 1-8, DOI: 10.5815/ijcnis.2013.07.01