MANET: Black Hole Node Detection in AODV

Ms.Chetana Khetmal[1], Prof.Shailendra Kelkar[2], Mr.Nilesh Bhosale[3]
[1] M.E Student, Vidyalankar Institute of Technology,Mumbai, [2] Asst.Prof. Vidyalankar Institute of Technology, Mumbai,
[3] Software Engineer, Oracle, Hydrabad.

ABSTRACT:

In today's world every user need to transfer data with one-other irrespective to individual's geographic location. Hence a Mobile Ad-hoc Network (MANET) has become a vital part of modern communication over wireless network. MANET helps to transfer data without fixed infrastructure and many autonomous nodes vigorously can become part of ongoing communication. Due to this, MANET gets attacked by malicious nodes very easily. Hence secure routing of data packet in MANET is essential task. There are number of attacks we have seen in MANET like Denial of Service attack, Jellyfish attack, Warm-Hole attack etc. In this paper we are concentrating on Black Hole attack in AODV i.e. Ad-hoc On Demand Distance Vector Routing. We are proposing authentication techniques based on Authenticated Node, Authentication on Path, Authentication Key Packet and Data Routing Information table (DRI) on each node.

By using authentication techniques we are trying to detect black hole in network so that we can transfer data packet over secure path.

KEYWORDS: *AODV routing protocol, Authentication Terminologies, Black Hole Attack, MANET (Mobile Ad-hoc NETwork), External or Internal attack, Active or Passive attack.*

I. INTRODUCTION

Wireless applications and devices(Laptops, Cell phones, Personal Computers etc) have mainly two modes of operations; one is in the presence of Control Module (CM) called as *Base Stations* and second is *Ad-Hoc connectivity* where there is no Control Module involved. The devices belong to wireless network exchanges data with each other without any wired connection between them. For communication between mobile devices, these nodes should belong to the transmission range of each other; if there is no direct connection from source to destination than intermediate nodes assist for transmission using hop by hop connections. Ad-hoc network having various characteristics [1] like non- infrastructure, autonomous node, dynamic in nature, scalable and many more which causes MANET to become popular in this modern era.

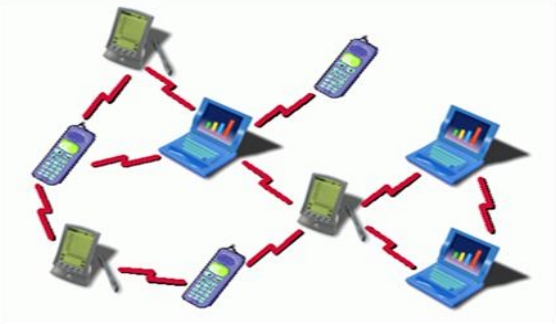


Figure 1. Mobile Ad-hoc NETwork

Mobile Ad-Hoc networks are full of *autonomous nodes* i.e. the nodes which are not having any central control node for their management. Due to the mobility of devices *dynamic topology* appears in wireless network. Communication can be carried out with mutual understanding among the nodes. There is no any restriction on

mobile node for leaving and entering in the network. These autonomous nodes can act as host/router or both at the same time. A *host* which demands for particular services from other nodes and a *router* node helps to forward the data to the neighboring nodes also discovering and maintaining routes for other nodes. The mobile

nodes have *self-configuration* ability due to which they can organize themselves in any network without prior infrastructure. Ad-hoc networking is applied on battlefield or for military units where static infrastructure is impossible and stills the communication among the users within a transmission range is necessary [3].The Attributes of MANET like changing topology, lack of central monitoring and management, no security mechanisms, limited battery and open medium where all nodes can access data within the communication range without any transmission medium between them; any un trusted node can become part of ongoing communication and demolish current packet transmission by dropping the packets, by changing the data from packet headers or by presenting wrong information to the network. Hence MANET is enormously prone to get attacked by malicious nodes.

II. COMMUNICATION IN MANET

In MANET communication takes place using TCP/IP structure among its mobile users. Therefore traditional TCP/IP has been modified to achieve betterment in transmission [3].There are various routing protocols which are use to route the packet securely from source to destination over the communication channel. The protocols like AODV (Ad-hoc On Demand Distance Vector), DSR (Dynamic Source Routing), DSDV (Destination Sequenced Distance Vector) etc are some routing protocols which are useful over wireless communication. Major aim of routing protocol is to establish shortest path (i.e. with minimum hop count) between source and destination nodes also less bandwidth to be used to traverse packets in timely manner.Routing protocols in MANETs are organized into three different categories according to their functionality. The categories and the name of protocols in each category are listed down in Fig. 2:

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

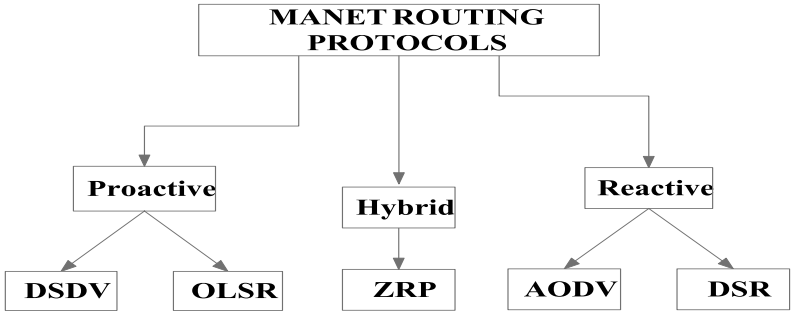


Figure 2. MANET routing protocols

1) Reactive Protocols:

Reactive protocols are known as *On Demand protocols*. These protocols are called reactive because they do not initiate route discovery by their own until any source node in the network request to find a route. These protocols setup routes when packet transmission demanded by users in the network.

2) Proactive Protocols:

A proactive protocol constantly maintains the updated topology of the network. Every node in the network knows about their neighboring nodes in advance. The routing information tables are maintained on each node and which are updated periodically. Whenever there is a change in the network topology, these tables are updated. The nodes exchange topology information with each other; any time when they needed.

3) Hybrid Protocols:

Hybrid protocol; it is a combination of strengthens of reactive and proactive protocol. It gives better results of transmission in MANET compare to other two protocols. It uses reactive or proactive approach as per the requirement of zones since it divides whole network in the small zones.

III. ATTACKS IN MANET

There are some flaws in MANET like [6]: No secure boundaries, No central management, Problem of scalability, Limited Resources, Dynamic topology, where it is hard to find out malicious nodes. Due to all this defects there are two main categories of attack one based *on the source of attack* i.e. External or Internal and other is based *on behavior of attack* i.e. Active or Passive [7]. In the fig. 3 and Fig.4 the circle represents different nodes in network which is shown by rectangle.

3.1.External and Internal Attacks: As shown in Fig 3 respectively;
External attacks: An External attacker from outside the networks tries to get access to the current network and once it becomes part of the network start interrupting ongoing transmission and performance of the whole network. External attacks can be prevented by implementing firewall, where the access of unauthorized person to the network can be avoided.

Internal attack: An attacker node is already works as internal node of network and also contributes in normal network activities. But after some transmission this node starts its malicious behavior. It is difficult to find internal malicious node of the network hence Internal attack is rigorous than external attack.

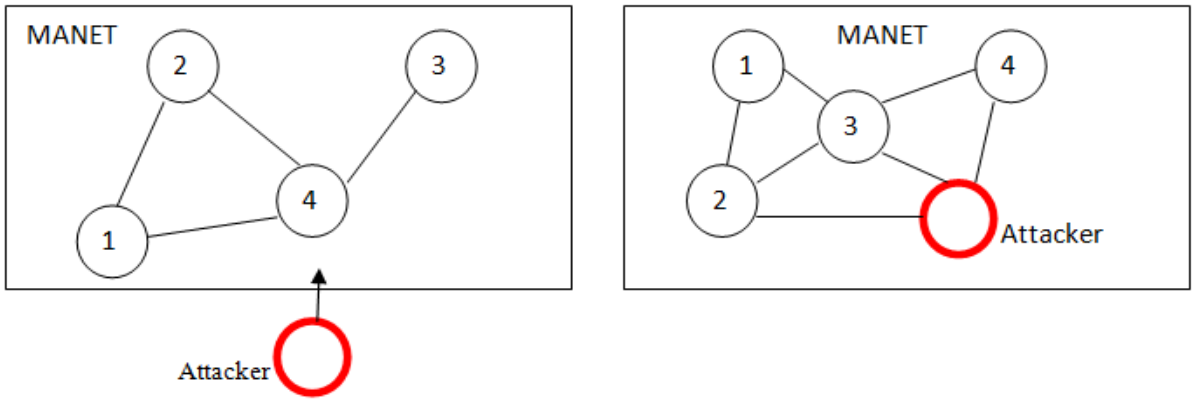


Figure 3. External and Internal attacks in MANET

3.2.Active and Passive Attacks: As Shown in Fig.4 respectively;
Active attack: It can be external or internal type attack. Being part of active network a node can destroy ongoing transmission by changing data, by stealing data or by denial of service.
Passive attack: In this attack the node does not introduce attack before getting the enough information about current network. The attacker node first observes whole network carefully by considering points like how nodes are communicating, what are the positions of the nodes.

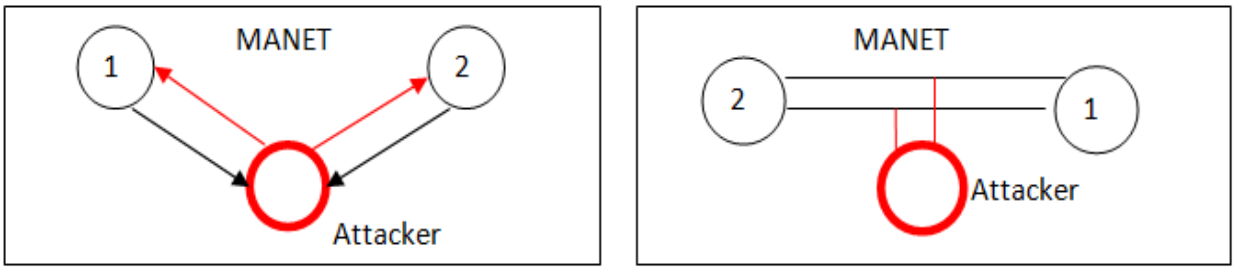


Figure 4. Active and Passive attacks in MANET

IV. BLACK HOLE ATTACK IN MANET

Black Hole is considered as an inside attack occurs in Network Layer and which is hard to find out also due to malicious node many damages takes place in the network [1] [4]. A black hole node sends fake routing information, claiming that it has an optimum route to reach to the destination requested by the source node and directs other good nodes to route data packets through it and consumes the transferred packets. Some major destruction generated by Black Hole is listed below:

- It increases network overhead; Due to unwanted transmission.
- It decreases the network's lifetime by boosting energy consumption unnecessarily.
- It destroys the network by dropping the critical data packets over the current communication channel.

As shown in Fig.5 the network having one black hole node; which shows fake route from source to destination and due to which the transmission error occurs and causes hazard in the mobile Ad-hoc network.

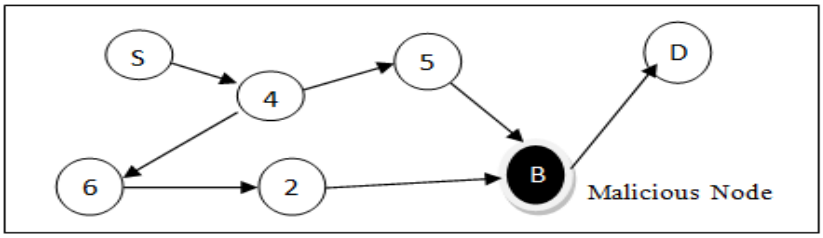


Figure 5. Black Hole in MANET

V. PROPOSED AUTHENTICATION TERMINOLOGIES

In our proposed system we are using AODV protocol and also different terminologies which help us to determined black hole in the network. We will work on it as reactive technique.

5.1. AODV (Ad-hoc On Demand Distance Vector) Protocol [7]

It is On Demand reactive protocol. It uses three types of messages: explained using Fig 6

[1] RREQ (Route REQuest): Source node which wants to communicate with destination node broadcasts RREQ message. Each RREQ packet has TTL (Time To Live) value which gives idea about how many hops needs to be traverse. Some fields of Route Request message packets are shown below;

Route Request TableFileds

Source_ address	Source_ sequence	Destination_ address	Destination_ sequence	Broadcast_ ID	Hop_count

[2] RREP (Route REPly): A node which has requested identity or which has information about it generates RREP message and unicast it using the reverse path which was generated at the time of RREQ to reach the initiator of this request. Some fields of Route Reply message packet are shown below;

Route Reply TableFileds

Source_ address	Destination_ address	Destination_ sequence	Hop_count	Time to Live (Lifetime)

[3] RERR (Route ERRor): Every node in the network periodically keeps updating its routing table by checking status of its neighboring nodes. If any node found its neighbor is down than it generates RERR message to update other nodes in the network.

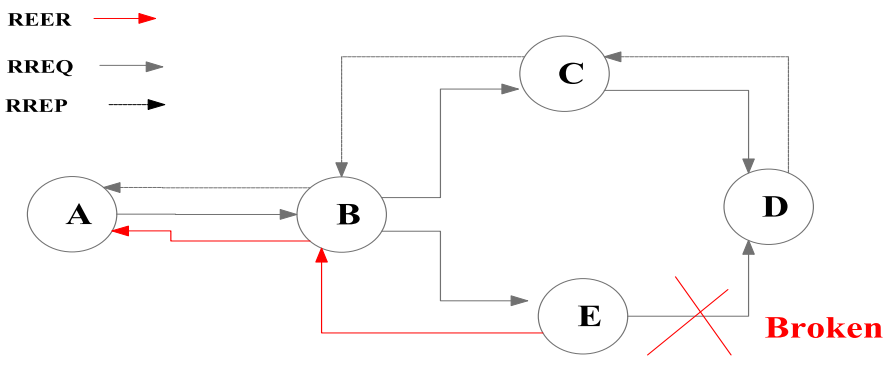


Figure 6. AODV protocol transmission with all type of messages

5.2. Proposed Terminologies

Following are some terminologies which we are using to transfer our very first data packet over the network using AODV protocol.

5.2.1 Authenticated Node (Authn)

If any node has already done successful transmission via its immediate node than the status of its Authn will be True. It means that path is secure for further transmission in same period.

As shown in Fig.7 **Authn(X,Y)** Sender : Node X Receiver : Node Y

Node Y is authenticated to Node X; it means Node X has at least one successful transmission completed through Node Y.

Hence Authn(X,Y) = T else Authn(X,Y) = F

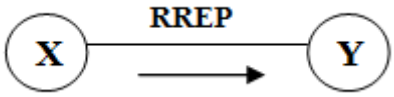


Figure 7. Transmission between Node X and Node Y

5.2.2. Authentication on Path (Authp):

When we are not getting an authentication of required neighbouring node that time we should carry Authentication of Path. We have to choose immediate neighbours of current node and if only one node is available than by considering mutual trust without waiting for any other option directly transfer packet to that node.

As shown in Fig.7 **Authp(X,Y)** **If Authn(X,Y) = F then Authp is carried out.**

Choose all path from Node Y i.e. Set of all Pi

If Pi = { } Then send to exact next node

5.2.3. Auth Key Packet (Authkey):

It is a packet used for authentication of destination. When intermediate nodes receives RREP message from any source node; the intermediate nodes will forward the acknowledgement packet along with some authentication majors. The authentication will be done using security questions or more information to authenticate the nodes on the route. We are considering MAC Address and also we will see Data Routing Information of each node along with normal routing table [3][6].In DRI table we will add the fields like node and the transmission taken *Through and From* that node. The DRI table will be updated periodically.

5.2.4. Acknowledgement:

After successful completion of first data packet acknowledgement is sent back to the source node.
If Ack = success

Ack(sucess) = {Ack 0, info of Authn(X,Y)}

If Transmission between Node X and Node Y is successful than ack will be sent to Node X also the status of Auth(X, Y) will be updated.

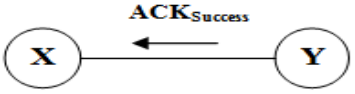
If  **Than updated Auth(X,Y) = T**

Figure 7. Successful transmission through Node X to Node Y

After following these steps source will receive Authkey packet from all the nodes which are on its path.

If Authkey packet differs considering its security means then the Black hole is detected.

Else data packet can be passed from the path.

5.3. Example for detection of Black hole using above technologies:

As shown in the following network; there are total six nodes which are connected.

Source Node = A Destination Node = D

Let; Authn(A,B) = T Authn(F,D) = T Means Successful data transmission already occurred.

Authn(B,C) = F Authn(C,F) = F Means Still any successful data transmission not occurred.

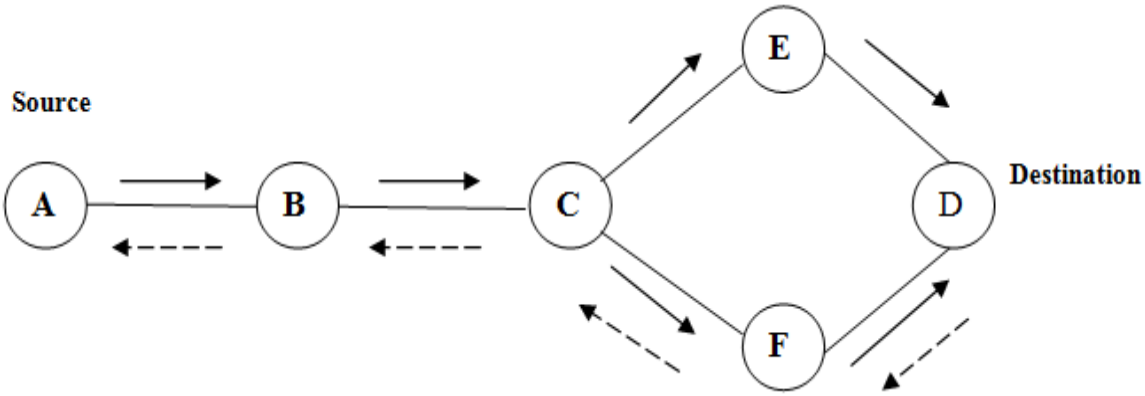


Figure 8. MANET Example with our Terminologies

Some notations we have used like:

Steps for solving:

1. Initial data packet transmission is initiated from source Node A.
2. Since Authn(A,B) = T

   Pass packet to Node B
3. Since Authn(B,C) = F we will go for Authp(B,C)

   Also $P_{B\ TO\ D} = \{ 0 \}$

   No other authenticated path exists from Node B hence pass packet to Node C by considering mutual trust.
4. Authn(C,F) = F and Authn(C,E) = F Hence consider Authp

   Since $P_{C\ TO\ D} = \{CFD,CED\}$ Hence send packet to both the path.

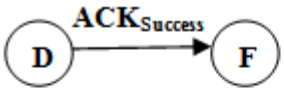
   After getting reply of Autkey packet from Node F and Node E.

5. Since Authn(F,D) = T

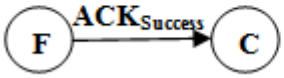
   Pass packet to F by considering Authp(C,F) and then Pass packet to D.

6. After successful transmission of data packet from Node A to Node B; routing tables of receiving nodes are updated.

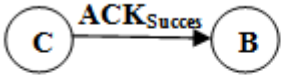
7. If there is any changes seen in authentication packet than that node can be consider as Black Hole in the network.



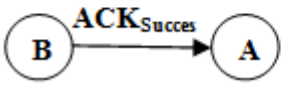
Node F updates its Authentication as; **Auth (F,D) = T**



Node C updates its Authentication as; **Auth (C,F) = T**



Node B updates its Authentication as; Auth **(B,C) = T**



Node B updates its Authentication as; Auth **(B,C) = T**

VI. CONCLUSION

Security of MANET is one of the vital features for its deployment. In our proposed system, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with black hole detection technique. Although there are many solutions have been proposed but still these solutions are not perfect. If any solution works well in the presence of single malicious node, we cannot guarantee about its usefulness in case of multiple malicious nodes. By using our new terminologies ; we are trying to discover and analyze the impact of Black Hole attack in MANET using AODV. Our terminologies will help to detect malicious node. Using authentication techniques as mentioned above we are able to forward data packets over secure path to the intended destination.

VII. FUTURE WORK

In Future the aim is to build up simulations to analyze the performance of the proposed solutions using NS-2.34. After successful implementation of AODV protocol we will try to compare performances of other protocols like DSR, DSDV, TORA etc using proposed terminologies. We will consider parameters for study like end-to-end delivery, Packet loss etc by varying the number of nodes and also the pause time in simulation environment.

REFERENCES

[1] Ms.Nidhi Sharma, Ms.Nidhi Sharma, The Black-hole node attack in MANET, Second International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4640-7/12 © 2012 IEEE.

[2] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[4] Rutvij Jhaveri,Ashish Patel,Jatin Parmar,Bhavin Shah, "MANET Routing Protocols AND Wormhole Attack in against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[5] Akanksha Saini, Harish Kumar," COMPARISON BETWEEN VARIOUS BLACK HOLE DETECTION TECHNIQUES IN MANET", NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.

[6] Akanksha Saini, Harish Kumar," Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Issue 2, December 2010 I S S N : 2 2 2 9 - 4 3 3 3 (P r i n t) | I S S N : 0 9 7 6 - 8 4 9 1 (On l i n e).

[7] IRSHAD ULLAH ,SHOAIB UR REHMAN, Analysis of Black Hole Attack on MANETs, Using Different MANET Routing Protocols, School of Computing,, Bleking Institute of Technology, June 2010