International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 5 (June 2014) http://ijirae.com

AN ANALYSIS FOR RECOGNITION AND CONFISCATION OF BLACK HOLE IN MANETS

Pardeep Saini*
Computer sci. & engg. & YIET

Ravinder Chouhan
Computer sci.engg. & YIET

Abstract - An adhoc network is a collection of mobile nodes which form a temporary network. These are known as mobile adhoc networks (MANETS) and they lack a fixed infrastructure and hence, for communication, these use wireless links. This use of wireless links makes them susceptible to malicious attacks. Ad hoc On-demand Distance Vector routing (AODV) is a widely adopted network routing protocol for Mobile Ad hoc Network (MANET). The design of AODV, however, paid little attention to security considerations, hence resulting in the vulnerability of such MANET to the black hole attack. This paper discusses the AODV protocol suffering from black hole attack. A feedback solution is given to this problem which comparatively decreases the amount of packet loss in the network.

Keywords – AODV, black hole attack, Feedback solution, MANET, Packet loss.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. The major disadvantage is their limited bandwidth, memory, processing capabilities and open medium and these are more prone to malicious attacks. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET).
Mobile nodes usually cooperate and forward each other' packets so as to enable communication between them. But some of the hostile nodes deny doing so; such type of misbehaviour is known as packet dropping or black hole attack**.** There are various routing protocols which suffer from such an attack. Based on the routing information update mechanism, routing protocols in ad hoc wireless networks can be classified into three broad categories: Proactive (table-driven) protocols, reactive (on demand) protocols, and Hybrid routing protocols.

One such is AODV which consists of two phases: route discovery and route maintenance. This paper discusses AODV and how black hole in a network following AODV affects the performance of the network.

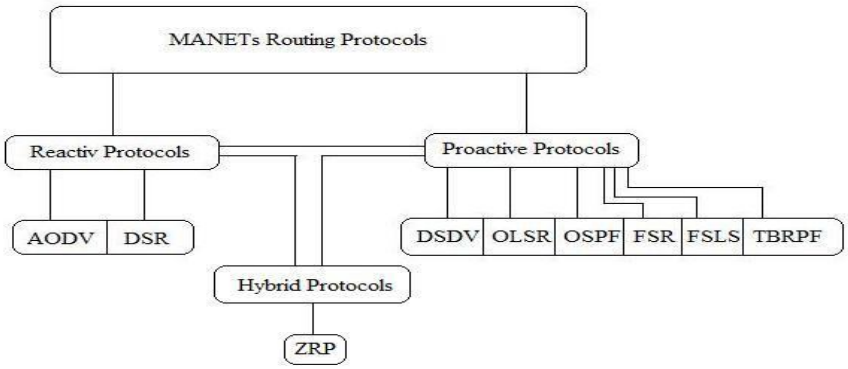

Figure 1 - Types of routing protocols

II. AODV ROUTING PROTOCOL

AODV is on demand driven protocol whose route discovery process is also reactive on an *as needed* basis. It works in two phases:

1. Route discovery phase
2. Route maintenance phase

It uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in. In route discovery process, the source node sends RREQ packets to all its immediate neighbours. If any of the immediate neighbours is the destination node, the corresponding node sends RREP packet to the sender node. In the other case, the nodes check whether it has entry for the route to the destination in their routing table. If yes, they send the route request RREQ to their further neighbours. This process will continue until the destination node or an intermediate node having a fresh route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbours. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbours. If the number in the routing table 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. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. In route maintenance phase, if during the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes.

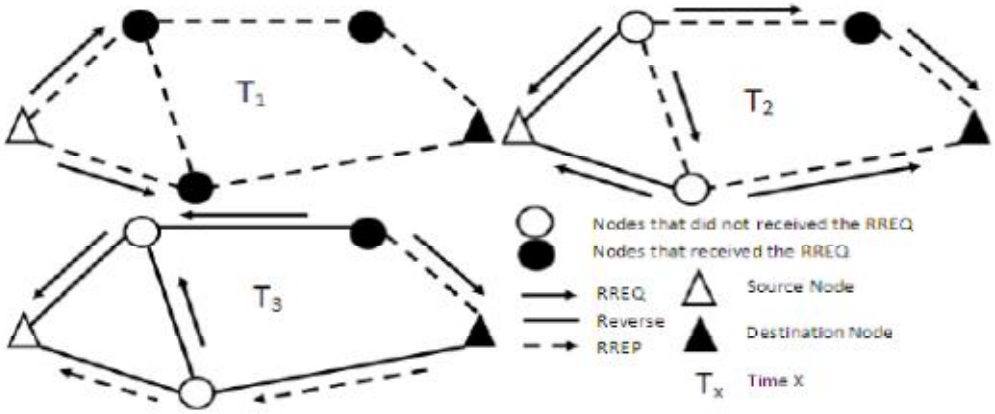

Fig. 2 Route Discovery in AODV

A. *Black Hole Attack*

This attack effects on data packet forwarding and not on route maintenance. Black hole attack is a denial of service attack in which a malicious node can attract all the packets claiming a fresh enough route to the destination and dropping all the packets reaching at that node.

B. *The Problem*

When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighbouring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole reaches the source node, well ahead of the other RREPs.

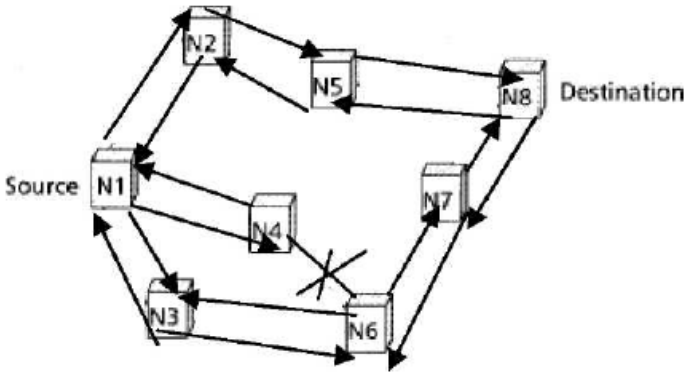

Figure 3 Behaviour of black hole in AODV

On getting the reply, the source node assumes that the process of route discovery is complete and it ignores further coming replies from other nodes. It selects the reply from the malicious node as the best route to send the messages using data packets. The reply sent from the malicious node has the highest sequence number which signifies the route to be the "fresh enough" and the source node relies on that reply. The attacker now drops all the packets coming to it. Let us consider the following example:

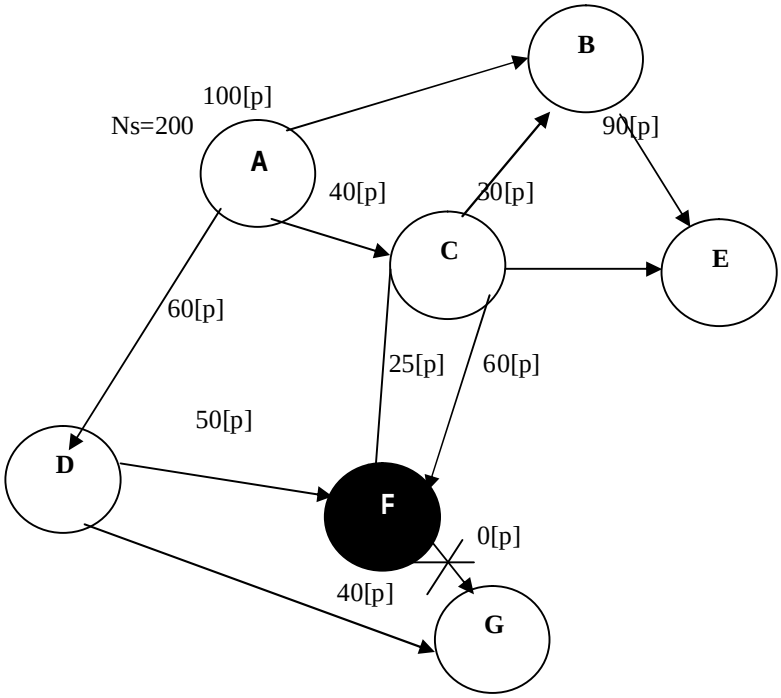

Fig. 4 Blackhole node

Here, node A is sending packets to node G. Node F does not contain any route to node G but it responds to A as if it has fresh enough route to node G. This node F is known as black hole node. All the packets sent by A destined for G are dropped by F. This is the problem in the network and in this paper proposes a solution to this problem named as feedback solution. The problem can be stated as follows:

Ns = Total no of packets sent by source A

Ns_{ij} = No of packets sent by node i to node j.

Let us consider,

$$Ns = 100 \quad (1)$$

$$N\,s_b = 100[p] \quad (2)$$

$$Ns_{ef} = 60[p] \quad (3)$$

As F is a black hole node, therefore,

$$\mathbf{Ns_{fg} = 0} \quad (4)$$

Nr = No of packets received at the destination G.
nr_j = no of packets received at node j
nr_{ji} = no of packets received at node j from node i.

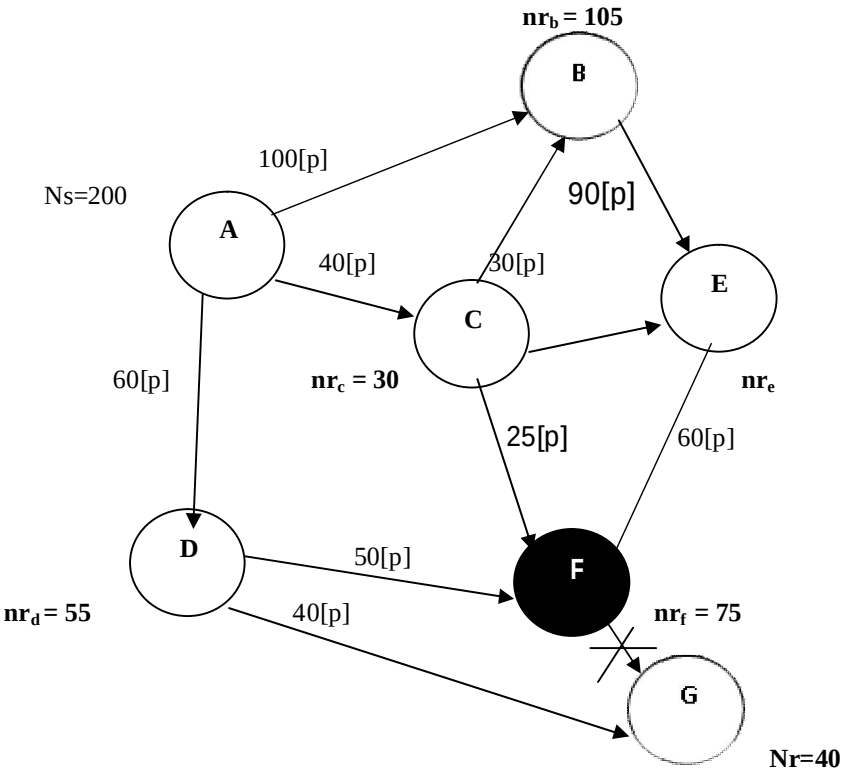

Fig. 5 No of packets received at G

From the above figure,

$$Nr_b = nr_{ba} + nr_{bc} \quad (5)$$

Let,

$$nr_{ba} = 80[p],\ nr_{bc} = 25[p] \quad (6)$$

$$Nr_b = 80[p] + 25[p] \quad (7)$$

$$Nrb = 105 \quad (8)$$

$$nr_{eb} = 100 \quad (9)$$

and as F is a black hole,

$$\mathbf{Nr_g = Nr = nr_{dg} = 40} \quad (10)$$

So as to solve this problem, following solution is proposed.

C. The Solution

One of the problems to this problem is to detect in the network, the blackholes by examining the no of sent packets at that node which will always be equal to zero for most of the cases. After the malicious black nodes have been detected we can adopt a feedback method to avoid the receptance of incoming packets at these blackholes. The packets coming at the immediate previous nodes to blacknodes are propagated back to the sender and the sender follows an alternative safer route to the destination.

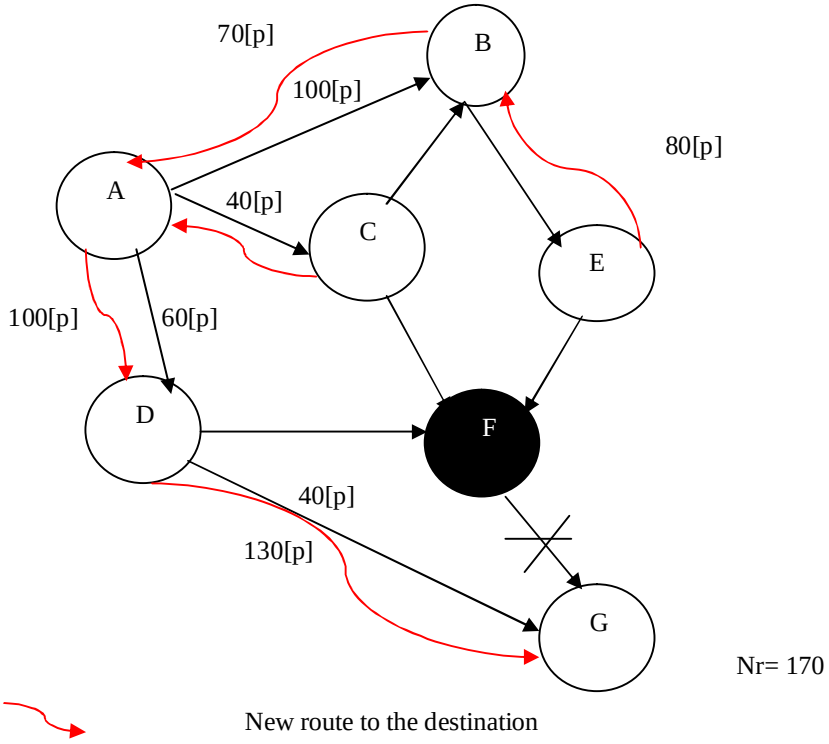

Fig. 5 Solution to black hole attack

1) *Result :* To calculate the amount of packet loss due to the presence of blackhole [5] in the network can be analysed as follows:

i) *Absence of black hole in the network:* Packet loss (%),

$$L = (Ns-Nr\ /Ns) *100 \quad (11)$$

$$L = ((200-175/200)) * 100 \quad (12)$$

$$L= 12.5\ \% \quad (13)$$

ii) Presence of black hole in the network:

$$L = ((200-40)/200) * 100 \quad (14)$$

$$L = 80\ \% \quad (15)$$

iii) When the solution is adopted :

$$L = ((200-170))/200)* 100 \quad (16)$$

$$L = 15\ \%$$

The above calculation shows that the presence of black hole effectively increases the amount of packet loss and by adopting the above solution; the packet loss can be decreased.

Further, the performance can be studied using the network simulator ns-2.

III CONCLUSION AND FUTURE WORK

In this paper we have presented a survey of the state of the art on securing MANETs against packet dropping attack. The problem is being discussed and a method has been proposed to eradicate the attack. But the analysis being done considers the network to be at an instance of time which may be considered as a static state. The solution is based on certain assumptions which are not always valid in the nature of mobile adhoc networks. The future work includes the mobility of nodes and considers the system to be dynamic in nature. The performance analysis shows that the amount of packet loss in case of presence of black hole is much more than that in the absence of such a node.

REFERENCES

[1] T. R. Andel and A. Yasinsac, *Surveying Security Analysis Techniques in MANET Routing Protocols, IEEE Commun. Surveys & Tutorials*, 9(4): 70-84, Fourth Quarter 2007.
[2] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "*Routing Security in Wireless Ad Hoc Networks*", University of Cincinnati, IEEE Communications magazine, October 2002.
[3] C. Perkins. "*(RFC)* request for Comments-*3561"*, Category: Experimental, Network, Working Group, July 2003.
[4] V. Karpijoki, "*Security in Ad Hoc Networks*", Seminar on Net Work Security, HUT TML 2000.
[5] B. Sun, Y. Guan, J. Chen and U. W.Pooch, "*Detecting black-hole attack in mobile ad hoc networks*", *Proc. 5th European Personal Mobile Communications Conference*, Apr 2003, pp. 490-495.
[6] I. Stamouli, "*Real-time intrusion detection for ad hoc networks*", Master's thesis, University of Dublin, September 2003.
[7] I. Stamouli, P. G. Argyroudis and H. Tewari, "*Real-time intrusion detection for ad hoc Networks*", *Sixth IEEE Intl Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05)*, 2005, pp. 374-380.
[8] Y. Huang, W. Fan, W. Lee and P. Yu, "*Cross-Feature analysis for detecting ad-hoc routing anomalies*", *Proc. of the 23rd IEEE Intl Conference on Distributed Computing Systems (ICDCS'03)*, May 2003.
[9] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "*Detecting blackhole attack on AODV-based mobile ad hoc networks by Dynamic Learning Method*", Intl Journal of Network Security, vol 5, no. 3, Nov. 2007, pp. 338-346.
[10] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "*Detecting blackhole attack on AODV-based mobile ad hoc networks by Dynamic Learning Method"*, Intl Journal of Network

