ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 2 (Apr. - Jun. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Avoiding Black Hole Attack Using Trust Based AODV Routing Protocol For Mobile Adhoc Network

[I]Muralidhar B.M, [II]Yuvaraju B.N
[I]M.Tech, Dept. of Information Science, The National Institute of Engineering, Mysuru, India
[II]Professor, Dept. of Computer Science, The National Institute of Engineering, Mysuru, India

Abstract
MANET refers to mobile adhoc network wherein, there is no fixed infrastructure. It's a temporary network consisting of multiple nodes which are allowed to cross the network as they are mobile in nature. The main issue in MANET is security. As MANET is wireless it is prone to attacks than wired network. Black Hole attack is most common in MANET. A Black Hole node pretends to be a trustworthy node which advertises itself as it has a shortest path to destination. In this paper we are proposing to solve the Black Hole attack by AODV Routing Protocol with Trust Control. This can be used to detect and prevent Black Hole attack in the network. The experimental results can be done using Java or NS2.

Keywords
MANET, AODV, MAODV, Black Hole Attack and Trust.

I. Introduction

MANET's spontaneously forms a wireless network consisting of cluster of mobile nodes. It may have nodes that are separated from the network. The devices that are used by adhoc network are PDA,laptops,cell phones etc. MANET faces more difficulty in providing security compared to wired and wirelessinfrastructure. The trust among the nodes will be difficult. Some of the security issues are

A) Authentication: To identify the sender's identity i.e. proof of the identity of the user logging on to some network.

B) Confidentiality: The information sent by the sender must be accessible by the authorized users only.

C) Integrity: Ensuring that the information is not altered by the unauthorized users in a way that is not detectable by authorized users.

D) Non-repudiation: Assurance that the claimed sender or recipient is in fact the party who sent or received a given message. Black Hole attack is considered to be one of the popular attacks in MANET. Security issues can also be found in DOS attack, poison attack, snooping, worm hole attack, gray hole attack etc. Some of the open issues are bandwidth, energy consumption, data delivery ratio, throughput etc. This paper is organized as follows: Section 2 describes AODV routing protocol. Section 3 describes black hole attack. Section 4 describes related work. Section 5 describes implementation. Finally conclusion and future enhancement.

II. AODV Routing Protocol

AODV refers to Adhoc on demand routing protocol. It's a reactive protocol which maintains routes of the nodes that needs to communicate.

To specify fresh route it uses Source Sequence number(SSN) or Destination Sequence number(DSN). It does not contain the whole route path instead contains the source and destination information. To establish the connection between source and destination it first sends the HELLO message and subsequently RREQ is sent to the neighbouring nodes. The RREQ is forwarded by the neighbouring nodes till the destination is reached. Once the path is established the nodes reply with a RREP message. If the acknowledgement is not received by the specified time again RREQ is sent. Once the path is established the data is sent to the destination.

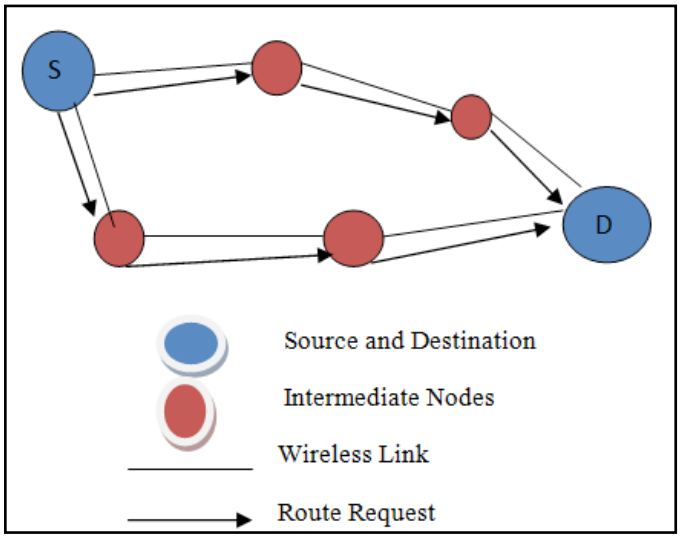

Fig 2.1: RREQ

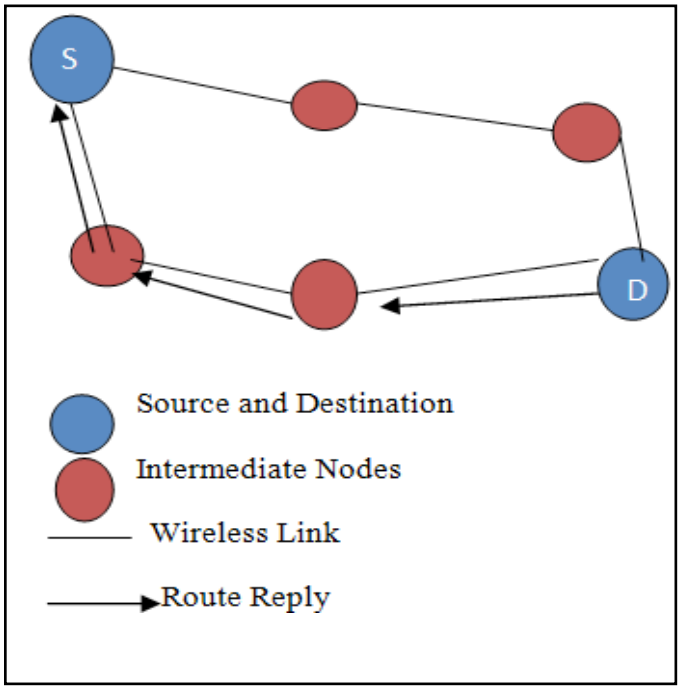

Fig 2.2: RREP

© All Rights Reserved, IJARCST 2013

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

This protocol provides an on demand Routing and it is rapid in nature. It uses node sequence numbers to differentiate between the newly arrived message or not.

Type	Flags	Reserved	Hop count
RREQ(broadcast) ID			
Destination IP Address			
Destination Sequence Number			
Original IP Address			
Original Sequence number			
ETL			

Fig 2.3: RREQ Message Format

Type	R	A	Reserved	Prefix	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Life time					
Hash Function	Message Digest				

Fig 2.4: RREP Message Format

III. Black-Hole Attack

The black hole attack problem has attached the attention of many researchers. Many algorithms have been proposed to solve this problem. These algorithms are either completely new stand-alone protocols, or in some casesincorporations of security mechanisms into existing protocols (e.g. AODV).As we will see, the design of these solutions focuses on providing countermeasures against black hole attack. In this section we introduce some of the existing algorithms used to avoid the black hole attack.

IV. Related Work

This paper proposes a specification based IDS that detects attacks on AODV protocol. To specify the exact routing behavior of AODV routing FSM is used. [1]

In [2] an additional field in the protocol message is proposed to enable monitoring. With the help of dynamic training method Anomaly detection scheme is used which updates training data at regular intervals of time assuming that the first RREP message is from black-hole node.

In [3] an efficient algorithm for preventing black-hole attack in AODV is proposed. This algorithm identifies the black-hole node by their sequence number. If the sequence number is larger than sequence number given by source node then it is considered as black-hole node. Once the malicious node is identified then it is updated in the routing table.

In [4] to solve selective black-hole attack in MANET that is based on Anti-black hole mechanism (ABM) an IDS is proposed. When the nodes perform ABM an estimation is done on the suspicious value of a node according to the abnormal difference between RREQ and RREP sent by the node. With an prerequisite that intermediate nodes do not reply to the RREQs and if an intermediate node that is not a destination node, never broadcast RREQs for a specific route then that nodes suspicious value increased by one. If the suspicious value of a node exceeds threshold a block message is broadcasted by the detected IDS to all the nodes in the network in order to isolate suspicious node.

V. Methodology

The configuration network takes the number of nodes as input and the configuration parameters are supplied to the simulator. The simulator consist the sink, node, and trust calculator for transmitting the packets over the network by using trust guided routing. It takes the configuration parameters. The sink is used to collect packet data from node and it also contains the packet delivery ratio. The trust value is calculated based on trust routing and best relay of network. The mobile ad-hoc network consists of collection of nodes and the data is transferred from source to destination node with the help of intermediate nodes. Based on trust value data packet takes trusted route to reach the destination node.

Pseudo Code:

Algorithm: sendPackets

```
input: srcnode , forward node
send count[srcnode][forward node]++;
forward Packet(forward node);
ack<-wait_for_ack
if (ack recieved)
{
success count[srcnode][forward node]++;
}
```

Algorithm: - Trust Calculation

```
for i=1:no of node
for j=1:no of node
Trust(i,j)= successcount(i,j)/sendcount(i,j)
End
End
```

Algorithm: Trust Based forwarding

```
input : packet at srcnode , target node
curr = srcnode
whilecurr != target node
nextnode<- get neighbour of curr with highest trust and shortest distance to target
curr= nexnode
end
```

VI. Results

MANETs are prone to security attacks. Many mechanisms has been proposed to solve the security attacks. In this paper trust calculation is done to avoid black-hole attack. The parameters such as throughput, packet delivery ratios etc. are done in this paper. The simulation results may be perform using a simulation tool. In trust based routing throughput and packet delivery ratio is far better compared to modified AODV.

© 2013, IJARCST All Rights Reserved

Fig. 6.1: Throughput

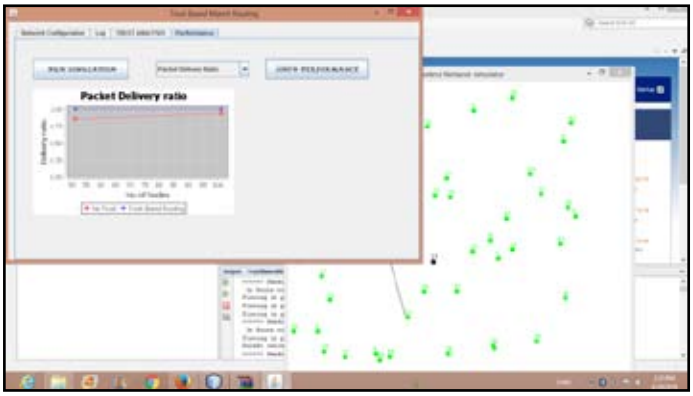

Fig. 6.2: Packet Delivery Ratio

Below figure no 6.3 and 6.4 shows the packet drop in between and the successful transmission of packet from source to destination in the presence of a black-hole node respectively.

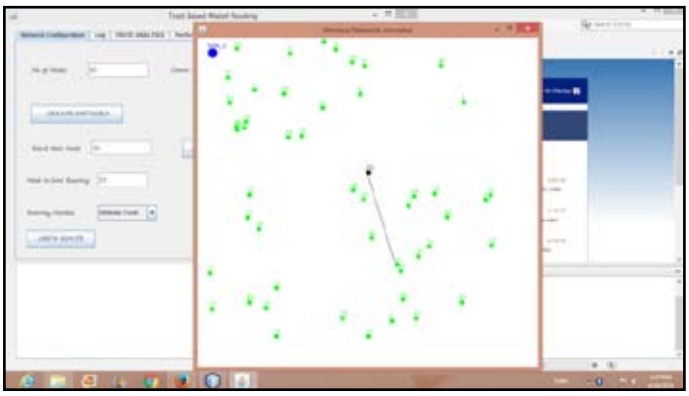

Fig. 6.3: Packet drop due to black-hole

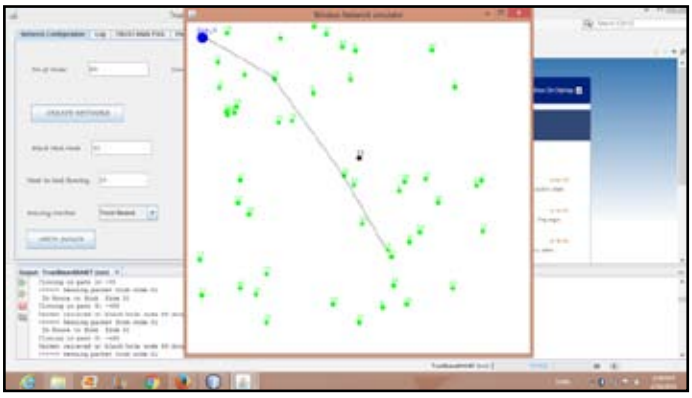

Fig. 6.4: Successful packet transmission

VII. Conclusion and Future Enhancement

Mobile ad hoc networks (MANETs) are dynamic wireless networks without any infrastructure. These networks are weak against many types of attacks; one of these attacks is the black hole attack. In this attack, a malicious node advertises that it has a freshest or shortest path to specific node to absorb packets to itself. In this paper, a modified AODV routing protocol is introduced to avoid the black hole attack in MANETs. Simulation results using NS-2 simulator depict the packet delivery ratio in the presence of malicious nodes. Three different scenarios for the black hole node(s) are applied; each one is implemented on protocol AODV. As a future work, the effect of other attacks such as wormhole and gray hole on the AODV and other routing protocols used in MANETs will be considered.

References

[1] *Tseng Chin-Yang, Balasubramanyam Poornima, and Ko Calvin, "A Specification-based Intrusion Detection System for AODV" in Proceedings of 1st ACM workshop on security of Ad Hoc and sensor networks, California, Davis, 2003, pp. 125-134.*

[2] *Sitapara Nishant and Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks," in International Conference on Emerging trends in engineering "ICETE-201O" , Jasingpur, 2010.*

[3] *Himral Lalit, Vig Vishal, and Chand Nagesh, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST), vol. 3, pp. 3927-3932, 2011.*

[4] *Yang Su Ming, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Elsevier Computer Communications, vol 34, pp. 107-117, 2011*

© All Rights Reserved, IJARCST 2013