International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

A Modified Method for Preventing Blackhole Attack in MANETS

Mukul Dhakate, Humera Khan, Prof. Anwarul Siddique
Department of Computer Science & Engineering, Rashtrasant Tukdoji Maharaj Nagpur University,
Nagpur, Maharashtra, India

ABSTRACT

Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's a real world analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue.

Study of previous work concludes that works done on security issues in MANET were based on different reactive routing protocol but still there is needs to avoid Black Hole attack in MANETs. This research work proposed detection and mitigation technique to avoid black hole attack and improve the network performance. Performance of proposed solution is similar with original AODV and tries to maintain privacy of content.

INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves.

To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

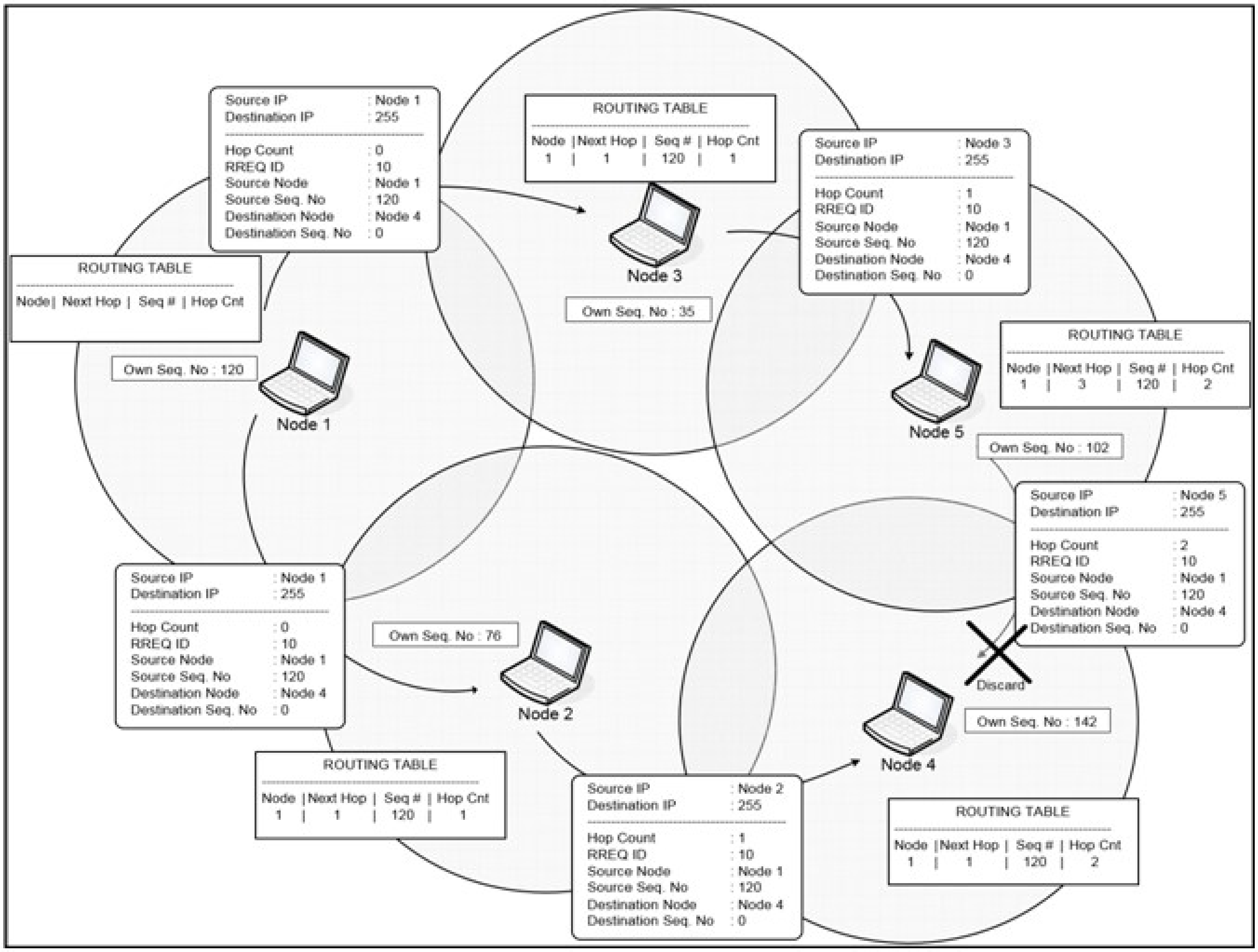
As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbour nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets.

In our study, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Black Hole attacks, we first added a new Black Hole protocol into the NS-2. We started our study by writing a new AODV protocol using C++, to simulate the Black Hole attack.

Having implemented a new routing protocol which simulates the black hole we performed tests on different topologies to compare the network performance with and without black holes in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a black hole.

Afterwards, we proposed an IDS solution to eliminate the Black Hole effects in the AODV network. We implemented the solution into the NS-2 and evaluated the results as we did in Black Hole implementation. As a result, our solution is eliminated the Black Hole effect with 24.38% success.

DIAGRAM:



ROUTING TABLE (Node 1)

Node	Next Hop	Seq #	Hop Cnt

Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE (Node 3)

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

Source IP : Node 3
Destination IP : 255
Hop Count : 1
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE (Node 5)

Node	Next Hop	Seq #	Hop Cnt
1	3	120	2

Source IP : Node 5
Destination IP : 255
Hop Count : 2
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE (Node 2)

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

Source IP : Node 2
Destination IP : 255
Hop Count : 1
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE (Node 4)

Node	Next Hop	Seq #	Hop Cnt
1	1	120	2

Fig (1). Propagation of the RREQ message

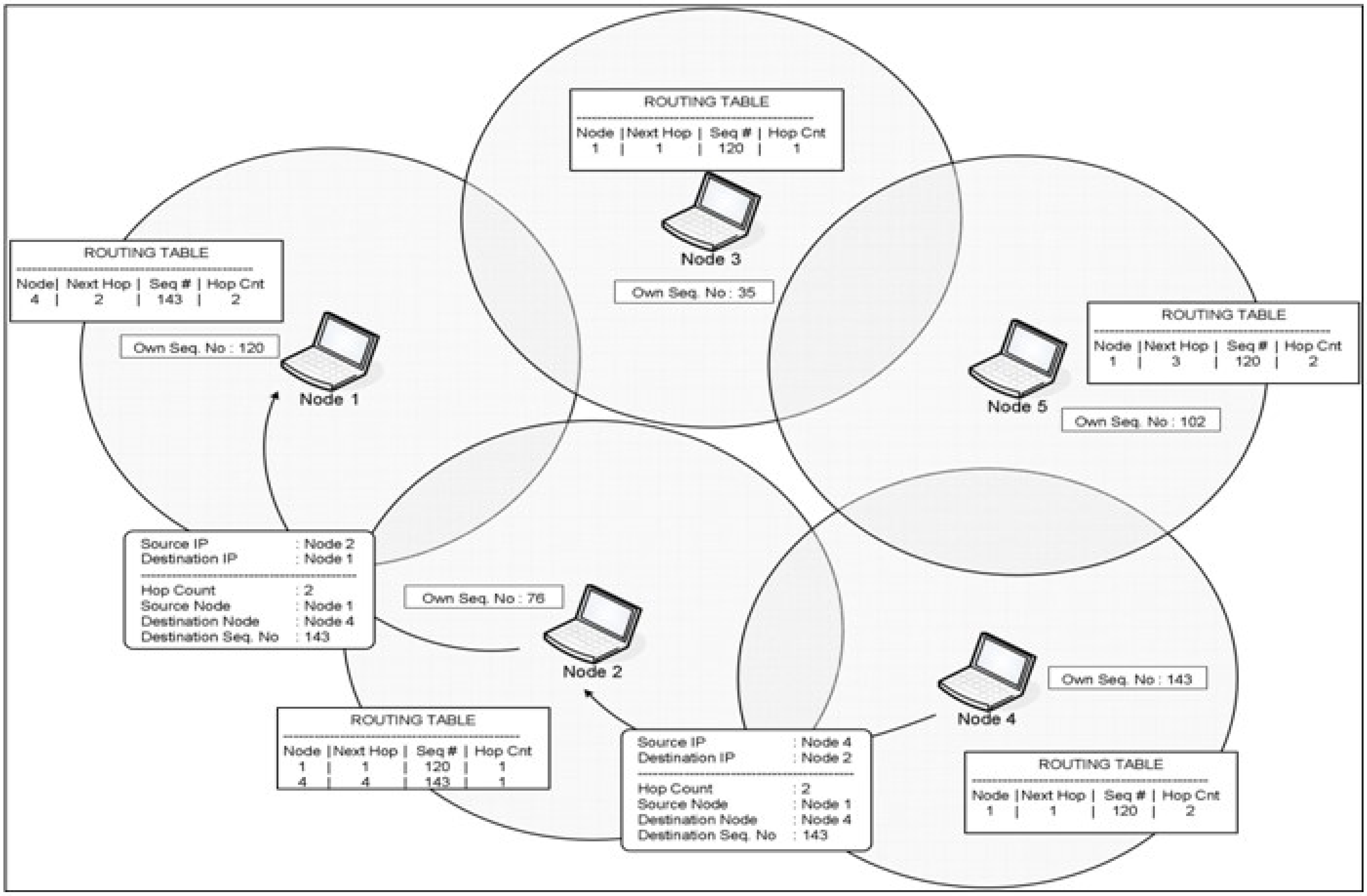


Figure 2 – Unicasting the RREP message

EXISTING SYSTEM

In the study, Conducted by Nath & chunky(2012).The researcher have tried to prevent a black hole in networking using the concept of clustering. The black hole comes in the path from source node to destination node According to the characteristic of the malicious node during black hole deployment node just receive data packet but never forwaded to destination node. Thus if server check only activity from sending & receiving packet then server is able to detect a malicious node. So,by doing this clustering it will be easy to server to check the node for the communication behaviour.I any node just receive just a data and it not forwarded any packet, then it will be suspect to the black hole node in the network.

However, the researcher have not provided any solution to detect the malicious cluster head the network and the internal malicious attacker the researcher have presented the detection and prevention scheme to study the effect of external malicious node entering in the network and in a internal node have been measured in trusted node. The attacker may cooperation some internal node in a network and get access the important information in a network. There getup a need to detect and prevent may malicious node present internally in an network including cluster head which can be compromised node present.

CONCLUSION:

In this study, we designed and implemented MANET using AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated scenarios which has 50 nodes that use AODV protocol and also simulated the same scenarios before introducing one Black Hole Node into the network.

Moreover, we are also proposing a solution that will attempt to reduce the Black Hole effects in NS-2 .

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis we have analyzed the behaviour and challenges of security threats in mobile ad hoc networks with solution finding technique.

Although many solutions has been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches our conclusion is that the approach offered by Deng suit well in our scenario. The intermediate reply messages if disabled leads to the delivery of message from destination node will not only improve the performance of network rather it will secure the network from Black Hole attack.

In our study we analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end to end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR.

ACKNOWLEDGEMENT

First, I would like to thank my guide **Prof. Anwarul Siddique** because of their guidance we are able to do our project successfully during the entire course.

I am also highly obliged to **Prof. M.S. Khatib**, Head, Computer Science and Engineering Department, for providing us with the help that would be contributing in our project. I would also thanks to honourable **Prof. Dr. Sajid Anwar**, Principal, A.C.E.T Nagpur.

Finally, I would like to thanks to all those who have contributed, directly or indirectly to make this project successful.

Prof. Anwarul Siddique

BOOK REFERENCES

1) H.Deng, W.Li and D.P.Agrawal, “Routing Security in Wireless Ad Hoc Networks,” University of Cincinnati, IEEE Communication Magzine, Oct, 2002

2) K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007

3) G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006

4) S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

5) Opnet Technologies, Inc. “Opnet Simulator,” Internet: www.opnet.com, date last viewed: 2010-05-05

6) S. Kurosawa et al., “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic”

7) M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf. 2004.