



NNA ALGORITHM TO PREVENT BLACKHOLE ATTACK

Chander Diwaker, Sunita Choudhary
CSE Department

University Institute of Engineering and Technology
Kurukshetra University, Kurukshetra
INDIA

Abstract: Mobile Ad hoc network is a collection of nodes which are self configuring and connected by wireless links automatically. One of the principle routing protocol used is AODV protocol. The security of AODV protocol is compromised by a particular type of attack called "Black hole attack". In this paper, we proposed Neighbor node analysis algorithm to prevent black hole attack which will provide a secure path that may be wider than shortest path. But it will provide high throughput and reduce the loss over the network. Computer simulation using NS2 shows that our algorithm provides better packet delivery, decreased packet loss rate and reduced packet delay.

Keywords: MANET, AODV, Black hole, NNA Algorithm

I. Introduction

The mobile ad hoc networks differ from existing networks by the fact that they depend on no fixed infrastructure. MANETs consist of nodes that are moving randomly with some speed. So MANETs have a dynamic topology. Due to lack of central monitoring system, these networks rely on mutual trust to carry out network operations. Each node in the network acts as both a host and a router[1]. Since mobile nodes communicate over a wireless channel, so the message security and transmission are the major concerns. Standard routing protocols such as AODV and DSR were designed without any security. Thus, these protocols are more vulnerable to different types of attacks.

A. Black Hole Attack

The Black hole attack is an active insider attack. It has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the nodes exploit the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. In other terms, a malicious node uses the routing protocol to advertise itself as having the shortest path to nodes whose packets it wants to intercept. In the case for AODV protocol, the attacker listens to request for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised. If the reply from malicious node reaches to the requesting node before the reply from the actual node, a fake route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to form a denial-of-service attack. In this paper, we focus on black hole attack [2].

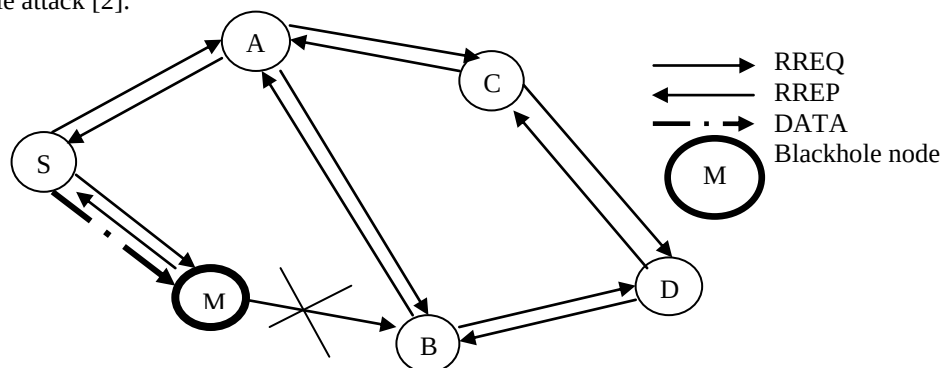


Fig. 1 Example of Blackhole Attack

In the figure 1, node M is a malicious node. When node S broadcasts a RREQ packet, nodes A and M receive it. Node M is a malicious node, thus it does not check its routing table whether it has the route to node D or not. It immediately sends back a RREP packet, claiming that it has shortest path to node D. Node S receives RREP

from node M ahead than RREP from node A. Thus, node S establishes path to node D through malicious node M and starts sending data packets. After receiving data packets from node A, malicious node M does not forward data packets; it simply drops all of the data or selectively forwards them. Thus the malicious node M behaves like a black hole. The rest of the paper is organised as follows: Section II introduces the proposed algorithm to detect the black hole attack. Section III shows the simulation results. Section IV concludes the paper and presents future work.

II. Proposed Work

We proposed neighbor node analysis algorithm to detect black hole attack. The proposed work is about detection of Blackhole Node attack between the communication taken place between the source and the destination. In this work, an authentication system is presented to detect and resolve the problem of Blackhole Node attack. In this work, each node is defined as an intelligent node that having the cryptographic algorithm implemented on it. As a node has to start the communication, it generates the neighbor nodes list and find the nearest neighbor. It generates a "hello" message and encrypts it by using the public key of the neighboring node. After the encryption, it passes the message to the neighboring nodes. As the neighboring node receives the message, it will perform the decryption using its own private key and then send the acknowledgement to the sender node back. If the neighbor node is not authenticated, it will remove its entry from the routing table and continue its work after updating the cache table. Immediate to this, it will transfer data to its most eligible next node. To check the eligibility of authenticated node, it will also observe some other factors like load on the node, response time etc. As the node reply, it checks if the response time is greater than its estimated response time, then it will again exclude that particular node from the list. There also exists some diagnostic algorithm to transfer the data with true decision making. The complete process is repeated node by node till the destination node is not achieved.

The Complete Algorithm is given here:

Newpath(S, D, N)

*/*S is the Source Node and D represents the Destination Node, N is the Size of Network */*

```
{
    1. Set Node S as the Current Node Cr
    2. Repeat the Steps till Cr!=Destination
    3. {
    4. Find the neighbor list (n0,n1...nM) from Node Cr
    5. Minload=Maximum
    6. For i=1 to M
    7. {
    8. If(Load(n(i))< Minload)
    9. {
    10. Minload =Load(n(i));
    11. j = i;
    12. }
    13. }
    14. If(Load(n(j))<THRESHOLD_LOAD)
    15. {
    16. Set n(j) as the Cr(Current Node) and goto Step 2
    17. }
    18. Else
    19. {
    20. Define Time T(1....THRESHOLD_TIME)
    21. Identify the Response Time
    22. If( ResponseTime <THRESHOLD_TIME)
    23. {
    24. Set THRESHOLD_TIME= ResponseTime
    25. Set THRESHOLD_LOAD = THRESHOLD_LOAD+1
    26. Goto Step 2 and Repeat the process
    27. }
    28. Else
    29. {
    30. Mark the node J as Black hole node.
    31. }
    32. } }
```

III. Simulation Results

The basic parameters of the proposed work are presented respective to the simulation environment in table 1. The system is implemented on Ubuntu Environment with NS2 simulator and XGraph is used as the tool for graph analysis.

Parameter	Value
Number of Nodes	36
Topography Dimension	800 m x 800 m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Packet Size	512
Mobility Model	Random Way Point
Antenna Type	Omni directional
Protocol	AODV

Table 1 Simulation Parameters

The mobile ad hoc network comprising of 36 mobile nodes is constructed in the NS-2 simulator in the topological boundary area of 800 m x 800 m. Figure 2 shows the network design.

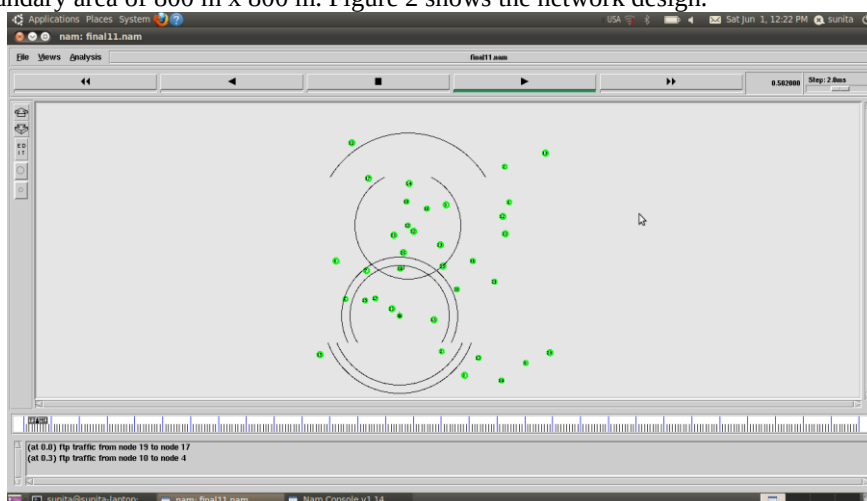


Fig. 2 Network Design

Now the simulation results of packet delivery, packet loss rate, bit rate, and packet delay rate are shown:-

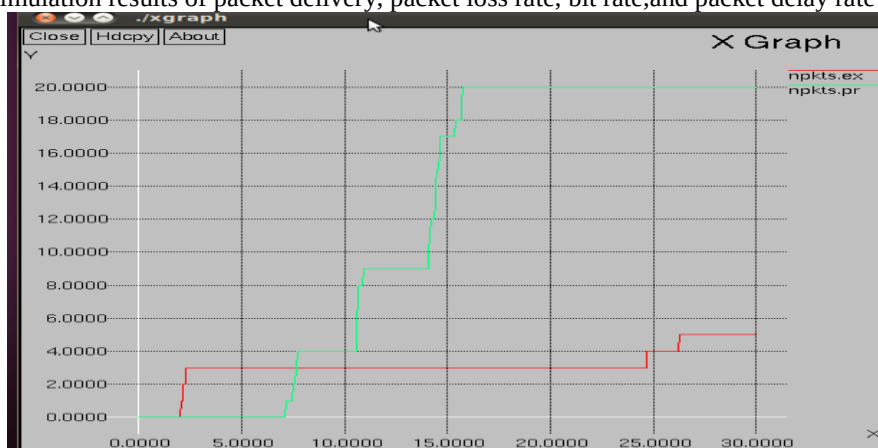


Fig. 3 Packet Transmitted (Existing Vs Proposed Approach)

Here figure 3 is showing the comparative analysis of packet transmitted over the network. Here x axis represents the time and y axis represents the packet transmitted. As we can see after implementing the proposed approach, the successful packet transmission over the network is increased.



Fig. 4 Packet Lost (Existing Vs Proposed Approach)

Here figure 4 is showing the comparative analysis of packet lost over the network. Here x axis represents the time and y axis represents the packet transmitted. As we can see after implementing the proposed approach the packet loss over the network is decreased.

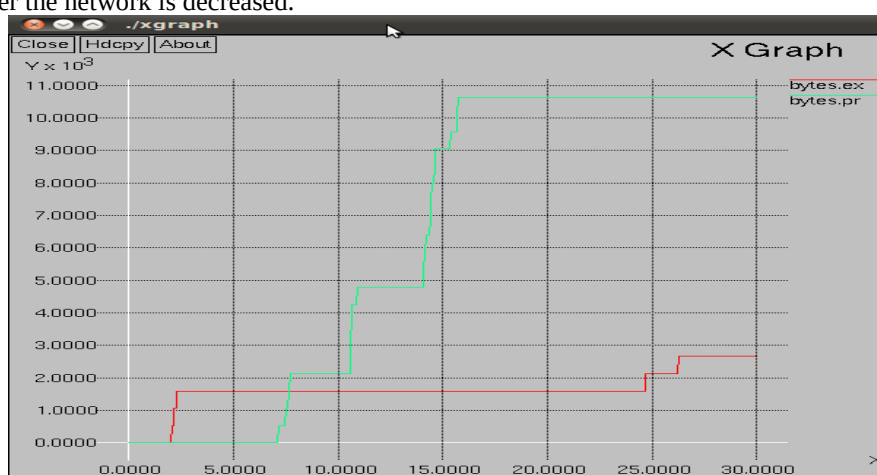


Fig. 5 Bytes transmitted (Existing Vs Proposed Approach)

Here figure.5 is showing the comparative analysis of bytes transmitted over the network. Here x axis represents the time and y axis represents the bytes transmitted. As we can see after implementing the proposed approach, the bytes transmitted over the network is increased.

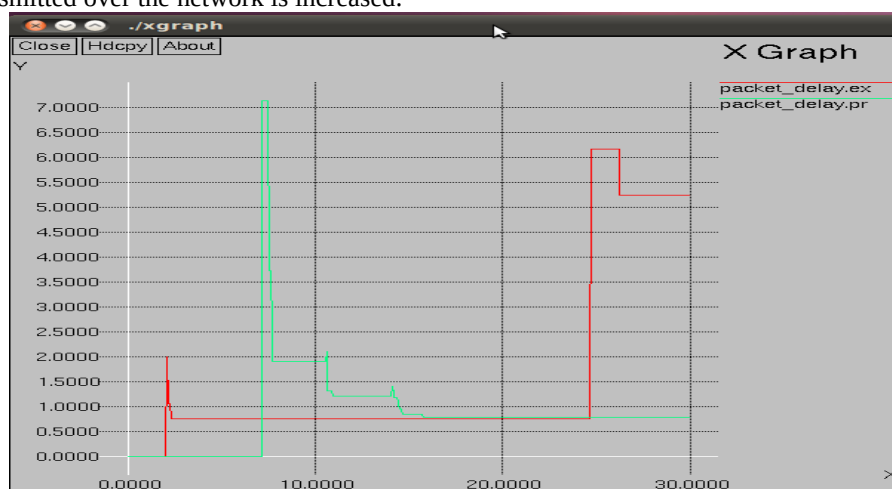


Fig. 6 Packet Delay (Existing Vs Proposed Approach)

Here figure 6 is showing the comparative analysis of Packet Delay over the network. Here x axis represents the time and y axis represents the Packet Delay of communication. As we can see after implementing the proposed approach, the Packet Delay over the network is decreased.

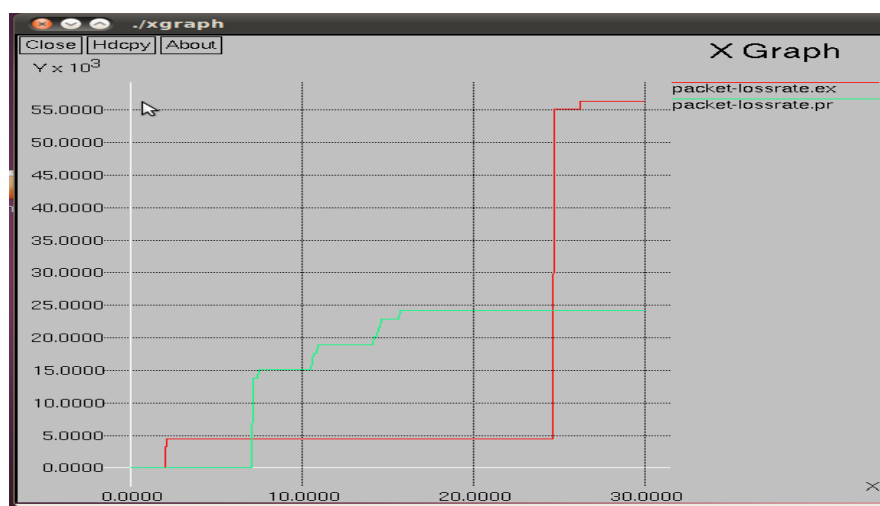


Fig. 7 Packet Loss rate (Existing Vs Proposed Approach)

Here figure 7 is showing the comparative analysis of Packet Loss rate over the network. Here x axis represents the time and y axis represents the Packet Loss rate of communication. As we can see after implementing the proposed approach, the Packet Loss rate over the network is increased.

IV. CONCLUSION AND FUTURE SCOPE

NNA algorithm is about the prevention of Blackhole Node attack. This is about to improve the AODV protocol in terms of security. NNA algorithm minimizes packet loss over the network and increases the throughput. The system is implemented in a wireless network with AODV protocol. Here we have proposed a new algorithm for the above said task. The implementation is performed in ns2 and analysis is presented using XGraph. The proposed system can be enhanced in future by other researchers in the following ways: (i) We have worked only with AODV protocol. The work can be implemented and analyzed along with other protocols, and (ii) We have performed the work only with Blackhole Node attack; the work can be enhanced by implementing some other attack such as wormhole, flooding attacks, DOS etc.

V. REFERENCES

1. Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks" In International Journal of Innovation, Management and Technology, Vol. 1, no. 3, ISSN: 2010-0248, 2010, pp. 279-285
2. Amit Goel, Doctor of Philosophy, "Moment-To-Moment Node Transition Awareness Protocol in a Wireless Distributed Environment" Submitted to YMCA Institute of Engineering, 2005
3. Anup Sahu, "difference between MANET and WSN", <http://www.scribd.com/doc/50634760/MANET-vs-WSN>, 2011, pp. 1-4 .