Remove the black-hole attack in mobile ADHOC network using Threshold Based Technique

Sanjay Yadav
M.Tech Scholar, Department CSE, TIEIT Bhopal, India
sanjayyadav787@gmail.com

Kaptan Singh
Department of CSE
TIEIT Bhopal, India
Kaptan2007@gmail.com

Abstract

In this paper enhanced the AODV routing protocol for the prevention of black hole attack. The enhanced AODV routing protocol based on the principle of thresholding. The thresholding using the concept of reference node selection process. The reference node selection process creates two group of node one is path altered group and other is stable path with sensibility. The sensibility path estimates the hop count and packet sequence number. If the number of hop count is not changed or the sequence of packet is also not lost is called sensitivity path of network. The function of threshold generated by the node distance formula based on the Euclidean distance derivation. The enhanced AODV protocol simulate in NS2.34 simulators and measure some standard parameter such as PDR, throughput, overload and E2E delivery ratio.

Keywords
MANET, AODV, Black-Hole, Threshold

Introduction

The malicious software attack such as black-hole attack and black-hole attack degraded the performance of mobile adhoc network and also theft the information of user. The black-hole attack denied the service of communication during the attacking mode. The detection and prevention of black-hole attack is various critical tasks. Various authors used various techniques such as threshold based function and reference based model for the detection of black-hole attack. In this dissertation improved the AODV routing protocol for the secured communication for the prevention of black hole attack. The prevention of black hole attack depends on the process of threshold based function. Initially threshold based function estimate the trust value for the request and replay process. The value of trust estimated by differential function. This differential function estimates the individual parameter selection value and reference value. For the detection process used reference selection process model. Threshold is an important part of the proposed technique. In the technique a black-hole tunnel present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the black-hole is detected. So accurate value of threshold is necessary for the technique. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the alternate route to its two hop neighbor that is called target node. The shortest path of minimum number of hop count of each and every alternate path is taken by the algorithm. After that the algorithm consider the highest number of hop count which is comes from these various alternate paths in the whole network and consider highest hop count + 2 as a threshold. The proposed protocol focuses on minimizing the routing overhead of the network. The worm of the link is determined by measuring received signal strength of RREQ packet using cross layer design and subtracting it from transmit power. A RREQ packet is only forwarded if the link has sufficient worm. So, the links with high worm i.e. weak links may not participate in formation of route. To decide whether the link has the sufficient worm or not, the worm of link is checked against a predetermined threshold. The threshold to be used can be a fixed value or it could be changing adaptively with changing network condition. Section II discusses about black hole attack Section III proposed method. Section IV discusses simulation finally, concluded in section V.

II. Black Hole Attack

The black-hole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the black-hole attack in MANET a technique has been proposed. In a black-hole attack, two attacker nodes join together. One attacker node receives packets at one point and "tunnels" them to another attacker node via a private network connection, and then replays them into the network [17]. The black-hole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node. When the neighbors of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process. This type of attack prevents other routes instead of the black-hole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed.
Proposed methodology

Threshold is an important part of the proposed technique. In the technique a black-hole present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the black-hole is detected. So accurate value of threshold is necessary for the technique. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the alternate route to its two hop neighbor that is called target node. The shortest path of minimum number of hop count of each and every alternate path is taken by the algorithm. After that the algorithm consider the highest number of hop count which is comes from these various alternate paths in the whole network and consider highest hop count + 2 as a threshold.

Assumptions

1. Total number of node in desire network is TN.
2. Si represent any node among TN, where i = 1,2,3,………..,< TN.
3. (RSi)j represent the node that’s come in the range of Si.
4. ((RSi)j)k represent the node that’s come in the range of (RSi)j and assume as a target node Tkj for Si.
5. P_ST represent path between S and T.
6. NSi represent the neighbor node of Si.
7. (lNSi,Tkj) represent number of node in the path PNSi,Tkj.

Algorithm

Step 1

If (i <= TN)
    Goto step 2
Else
    Threshold (T) = max (nH (PSi,Tkj)) + 2

Step 2

If (j <= n(RSi))
    Goto step 3
Else
    i++, goto step 1

Step 3

Set Si as a source node and determine (RSi)j

Figure 1: black-hole Attack scenario M1 and M2 two black node.
Step 4
If \((k \leq (n(RS)_{ij}))\)
Goto step 5
Else
\(J++\), goto step 2

Step 5
Determine \(((RS)_{ij})_k\) and set \(T_{jk} = ((RS)_{ij})_k\) as a target node for \(S_i\).

Step 6
Set \((PS_i, T_{jk})\) as a path

Step 7
Determine \(NS_i\) node and find route to there respective node \(T_{jk}\)
\((NS_i, T_{jk}) = l_{NS_i,T_{jk}}\)
And reply in term of number of nodes to \(S_i\)

Step 8
Source \(S_i\), select minimum \(l_{NS_i,T_{jk}}\) among all \((NS_i, T_{jk})\) and set
\(nH(PS_i, T_{jk}) = \min(l_{NS_i,T_{jk}})\)
\(k++\), goto step 4

---

**Figure 2:** proposed model of black-hole detection based on threshold based function
IV Simulation Result

To investigate the effectiveness of the proposed scheme for black hole detection in mobile adhoc network, the simulation on a simplified topology was carried out using Network Simulator version (ns-2.34)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation duration</td>
<td>100 sec</td>
</tr>
<tr>
<td>Simulation area</td>
<td>1000*1000</td>
</tr>
<tr>
<td>Number of mobile node</td>
<td>25</td>
</tr>
<tr>
<td>Traffic type</td>
<td>Cbr(udp)</td>
</tr>
<tr>
<td>Packet rate</td>
<td>4 packet/sec</td>
</tr>
<tr>
<td>Host pause time</td>
<td>10 sec</td>
</tr>
</tbody>
</table>

The packet delivery ratio can be determined by dividing number of packets received by number of packet sent[24]. This performance metric gives us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different traffic models.

The normalized routing load is the overhead on the network in order to find and maintain the route [23]. Normalized routing load can be determined by finding number of routing packets sent per number of data packet received, the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. In other words, it is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received [24].
Both the path loss sensitive variants of AODV does not process the RREQ if it is having large path loss, that will reduce the routing load in both the variants. The AODV does not have stable route which increases the route discovery. Increased route discovery incurs more routing overhead.

AODV has minimum no of hops so, there will be less time spent in processing the data packets. It is true that both SEAODV gives stable route but, they finds a route with increased no of hops compared to AODV which will increase the End to End delay compared to AODV. The increased End to End delay of both SEAODV is considered as a trade-off of our proposed work i.e. the price we are paying to achieve the stable path.

V conclusion & Future Scope

In this paper modified the AODV routing protocol for the detection of black-hole attack. The modified protocol is called secured protocol (SEAODV). The SEAODV protocol based on threshold based function. The threshold based function measure the distance of normal node and black-hole node. Our proposed algorithm is very efficient in compression in AODV routing protocol. For the evaluation of performance our modified protocol tested in different network scenario tested through simulations for different distributions of nodes and black-holes and different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent detection probabilities with few false alarms that depend on the value of threshold. The results of the proposed are batter then the previous approaches in order to detect the black-hole.

References:


