IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 2, Issue 1. (Mar. - Apr. 2015), PP 01-05
www.iosrjournals.org

Detection and Removal of Blackhole Attack Using Handshake Mechanism in MANET and VANET

K.R.Viswa Jhananie[1], Dr.C.Chandrasekar[2]
[1]*Department of computer science, Indo Asian Women's Degree college, Bangalore,India*
[2]*Department of Computer Science, Periyar University, Salem, India*

Abstract: *MANET (Mobile Ad-hoc Network) do not require centralized or any infrastructure to form a network and so they are vulnerable to many attacks. Each device in MANET is free to move independently in any direction and therefore change its links to other devices frequently. VANET (Vehicular Ad-hoc Networks) is a type of MANET that is used for communication among vehicles and roadside equipment. Internet is used for transformation of data from vehicles. Black hole attack is one of the serious attacks in networks. In order to provide a secured network, we have given a solution for black hole attack using handshaking in MANETs and VANETs. We have chosen random way point model for MANET and city section mobility model for VANET. The simulation results using ns-2 for MANET shows effectiveness in securing messages than VANET. In this paper, we propose solution which will try to avoid black hole attack in network with the help of handshake mechanism that uses a periodic dynamic key value.*

Keywords: *blackhole attack, dynamic ID, handshake,MANET, VANET.*

I. Introduction

The Mobile Ad-hoc Network(MANET) is easy to deploy and since they are in mobile, they are very much useful in places where there is no proper network at all. They are used for communicating throughout the world while they are in mobile and places like military, and in any case of natural disaster. Vehicular Ad-hoc Network(VANET) is mostly used in fast moving vehicles. A vehicle that is VANET equipped will be able to receive and send information to the other VANET equipped vehicle. A vehicle is made VANET equipped by placing an electronic device in it which is used to form a network[1]. VANETs are used to provide safety for vehicles during traffic on road as well as to get weather information, to download music, to access internet, etc.

Since the nodes are moving, the topology of the nodes changes during the communication takes place. Since, the nodes change the path dynamically, the malicious node can easily introduce itself in any path and start absorbing all the data packets. To avoid this, we have used handshaking in network which is efficient. Handshake sets the parameter dynamically that is done before the communication channel is established between two entities. In this paper, we have used a handshaking mechanism which involves in verifying the dynamic id generated by our proposed algorithm.

Section-2 deals with random waypoint model and city section mobility model. Section-3 deals with AODV(Ad-hoc On demand Distance Vector) routing protocol and we discuss about black hole attack in Section-4. The methodology is given in Section-5. The related work on black hole attack is discussed in Section-6. The proposed solution is discussed in Section-7 followed by its algorithm in Section-8. The various simulation results are given in Section-9. The conclusion is given in Section-10 and the future enhancement is given.

1. Mobility Models:

1.1 Random Waypoint Model:

Random way point model is the most commonly used model for mobility. In random way point model,each node chooses its direction, speed and destination randomly independent of other nodes. Random waypoint model is synthetic, means it is not based on actual traces and limited to special geometry[2]. The mobility of the node is independent of the other node. Each node can move in any direction within its network region. The nodes are distributed randomly within the simulation area initially.

1.2 City Section Mobility Model:

City section mobility model, the nodes can move within the fixed boundary conditions. In this model, the network is assumed to be divided in to identical length of square blocks called grids. Since, the network has identical block length, the nodes will travel either in horizontal or in the vertical direction of streets formed by grids. A node has to choose a destination point in the street network. If the node has to move further in the network, it waits for a pause time and then again chooses the destination point in the street network[3].

2. AODV (Ad-hoc On Demand Distance Vector Protocol):

AODV is the most commonly used routing protocols used in MANET. It is one of the reactive protocols which maintains routing table. This protocol uses control messages to find the route from source to destination. (ie) RREQ (Route Request), RREP (Route Reply) and RERR (Route Error)[4]. A RREQ is sent from the source node to its neighbor node to forward the data packets to the destination. Once the neighbor nodes find a path, they will start sending RREP to the source node with the sequence number and hop count. When the next hop in the routing table entry breaks, all active neighbors are informed. Link failures are propagated with RERR which also update the destination sequence number. Whenever a connection is required, the source node sends RREQ message to its neighbor nodes in all paths. The neighbor node which exists in any path, after finding the route to its destination, sends a RREP message to the source node. RREQ has TTL(Time To Live) value which states the number of hops the RREQ should be transmitted. This is used to delete the entry when the intermediate node does not receive the RREP within the allocated time.

When any intermediate node in the route finds disconnection in its path, then RERR message is generated. All these above information is maintained in the routing table. Also, in AODV, each node maintains the next hop count information and destination sequence number. The routing table is updated only if the destination sequence number of the current packet received is greater or equal to the last destination sequence number stored at the node and it should have a shortest hop count. The routing table maintains source node ID, intermediate node ID, destination node ID and sequence number.

3. Blackhole Attack:

In blackhole attack, one node called as malicious node is involved in absorbing all the data packets from its neighboring nodes. A blackhole attack can be performed with a single node or more than one node (ie) cooperative attack. In this type of attack, the malicious node will introduce itself as a neighbor node by sending the fake reply to the source node with the highest sequence number[5]. It gives a fresh and recent route to the destination than the one previously known to the sender. With this RREP by the malicious node, the source node start sending all the data packets in this path and thus the communication between source node and destination node gets disconnected.

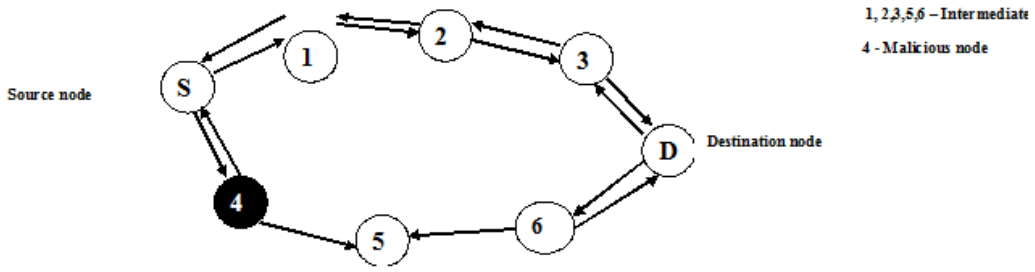


Fig 1: Black hole attack (single malicious node)

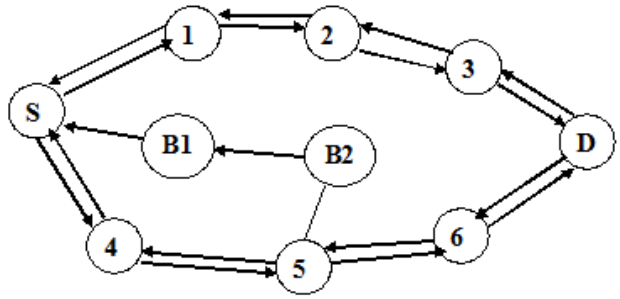


Fig 2: Cooperative black hole attack (more than one malicious node)

II. Methodology:

Theidea is to use handshake mechanism while forming routing table. Each node will generate periodic dynamic same value at the same time. When RREQ request send by the source, before adding the node into the routing table, it compares the handshake values of the node which says it knows the destination. Only if values

are same, that node will be added into the routing table as one of the nodes from source to destination else that node is identified as malicious node and ignored.

III. Related Work:

In [4], Satoshi et al has used a training method for high accuracy detection by updating the training data in every given time interval. In[5], Mohammad Al-Shurman et al have given a solution by using the sequence number. Since the next packet has a sequence number higher than the previous packet, the destination sequence number is checked with the other nodes. In [7], Juan- Carlos Ruiz et al Pedro Gil have discussed how to inject attacks in Mobile Ad-hoc Network. Palpanas et al. propose a model-based outlier detection algorithm in sensor networks. In their algorithm, normal behaviors are first characterized by predictive models, and then outliers can be detected as the deviations. In [9], sheenusharma et al has given a solution by using variable node mobility.

IV. Proposed Solution:

As mentioned above, Random Waypoint Model is taken for MANET and City Section Mobility model is taken for VANET. In Random Way Point model, the mobile nodes are initially distributed randomly around the simulation area [6]. In this model, each node chooses the next node uniformly in area, independent of past and present.

The network of VANET is thus basically composed of number of horizontal and vertical streets. Each street has two lanes, one for each direction (North/South direction for vertical streets, East/West direction for horizontal streets).

We have used handshake mechanism where a periodic dynamic Id (value) will be generated with the same value in all the nodes in the group which is involved in forwarding the data packet. Each node will forward the data packet within the allocated time to its neighboring node after verifying dynamic value. Since the malicious node does not belong to the group, the dynamic value will not match or know by malicious node[s]. Thus this route will avoid using that node for data forwarding.

V. Algorithm:

Step:1 path discovery process:
The source node S sends RREQ to its neighbor node in order to discover the path to the destination.
Step:2 developing the routing table:
A routing table is constructed with source Id, each intermediate node Id, destination Id and time taken by each node to forward the data packet to its neighboring node.
Step:3 verifying for trustworthy nodes (intermediate nodes)
Assume $\Delta t = 5ms$ where Δt is the sample time.
d_i= dynamic(first node), d_j=dynamic(second node)

$$d_i(t) = \sum_{j=1}^{N} d_{ij}(t)$$

where d_i is the dynamic id(value) of first node, d_j(value) is the dynamic id of the second node, N is the last node.
If($d_i == d_j \&\& d_{ij}(t) <= \Delta t$) then
Add the node to the routing table
Else
Malicious node.
Step:4 finding blackhole attack: (malicious node)
Repeat step:3untill data packet reaches destination node.

VI. Simulation Results:

As Expected, the simulation results show better performance in MANET where random way point model is used. Since the nodes do not have any restrictions in movement, it makes easy to forward the data packet. The nodes can move freely and can take sharp turns anywhere and in any direction in the path. In case of VANET, city section mobility model is used. In this, since the nodes have restrictions like, they can move only in horizontal and vertical direction and the turns can be taken only in the intersection of rows and columns. Because of the above constraint, the performance is little poor when compared to MANET. The various simulation results using ns-2 are given below:

End To End Delay(Less):

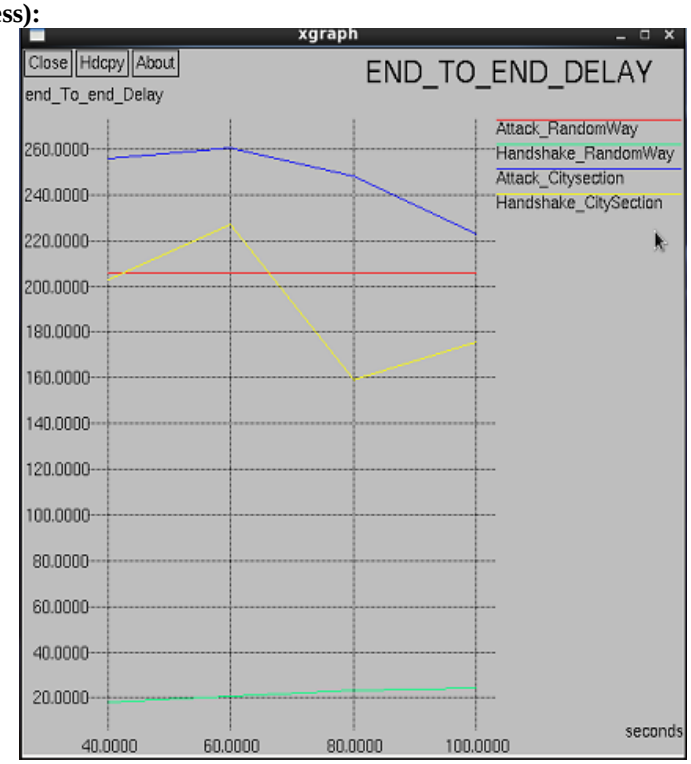
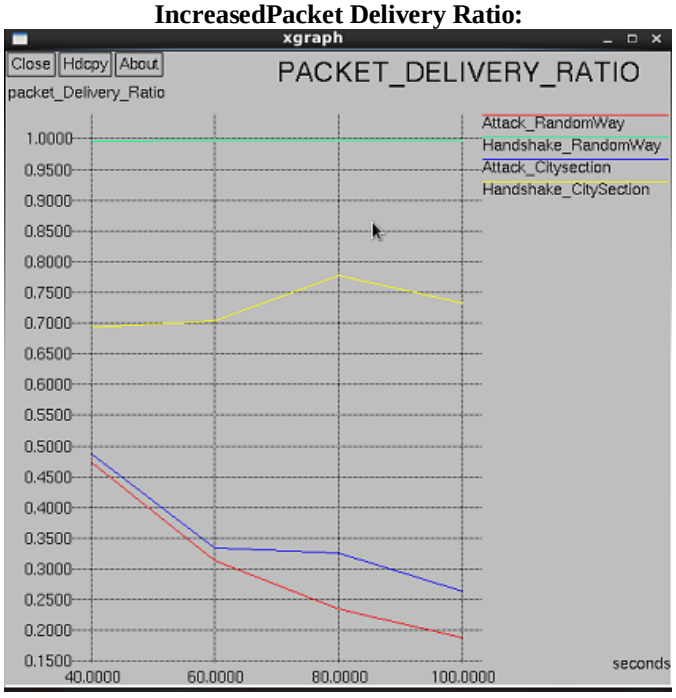
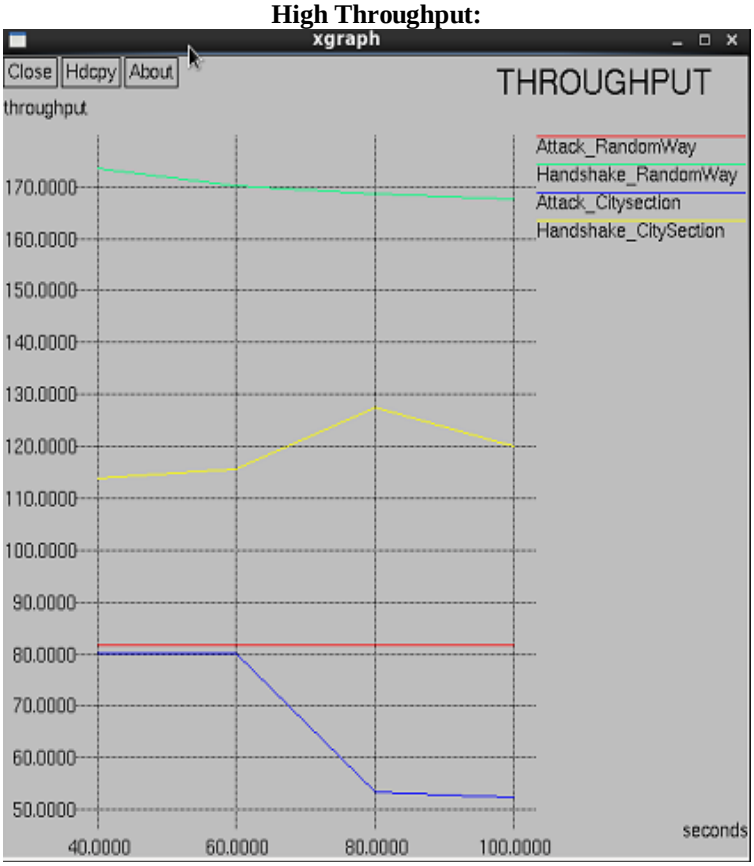


Fig (i)

IncreasedPacket Delivery Ratio:



High Throughput:



VII. Conclusion:

In our previous research paper, we have proved handshake mechanism as efficient. As an extension, in this paper, we have used handshake mechanism with a dynamic id in each node and a time period is given for each node within which the dynamic id should be verified and if it matches, the data packet has to be transferred. By doing this, not only the malicious node is identified, but also, the data packets reaches the destination without much delay. Our future work will be in finding a solution for co-operative nodes and for different attacks in MANET and VANET.

References:

[1]. NatarajanMeghanathan, "A simulation study on the impact of mobility models on network connectivity, hop count and life time routes for ad-hoc networks", Informatica(207-221).
[2]. E.Hyytia, H.Koskinen, P.Lassila, A.Penttinen and J.Virtamo, "Random waypoint model in wireless networks", Helsinki, 2005.
[3]. EmreAtsan and OznurOzkasap, "A classification and performance Comparison of mobility models for Ad hoc networks",Springer-Verlag Berlin, pp-444-457, 2006.
[4]. Sathoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipourand YoshiakiNemoto, "Detecting blackhole attack on AODV based Mobile Ad-hoc Networks by Dynamic Learning Method", IJNS,pp-338- 346, Nov-2007.
[5]. Mohammad Al-Shurman and Seong-Moo Yoo, SeungjinPark , "Blackhole attack in Mobile ad-hoc networks".
[6]. Christian Bettstetter and Christian Wagner, "The spatial node distribution of the random waypoint mobility model".
[7]. Juan-Carlos Ruiz, JesúsFriginal, David de-Andrés, Pedro Gil, "blackhole attack injection in adhoc networks".
[8]. Hao Yang et al., "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, Volume 11, Issue 1, Page(s): 38 – 47, Feb. 2004.
[9]. Sheenu Sharma and Roopam Gupta, "Simulation study of blackhole attack in the mobile adhoc networks", Journal of engineering Science and Technology, Vol-4, No.2 (2009) 243-250.
[10]. Web reference, "http://www.isi.edu/nsnam/ns".