Scientific Journal of Impact Factor (SJIF): 3.134

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 1, January -2016

Discovering of Wormhole Node by Hop-count and Delay

Gulzar Ahmad Wani[1], Dr Sanjay Jamwal[2]

[1]*Department of Computer Science, BGSB University, Rajouri*
[2]*Department of Computer Science, BGSB University, Rajouri*

Abstract—*In wireless Network, a decentralized type of wireless network called wireless ad-hoc network is a infrastructure less network i.e., it does not depend on existing infrastructure. Mobile Ad-hoc network (MANET) is a kind of wireless Adhoc network. MANET is a self-arranging, infrastructure less and decentralized network consists of two or more mobile devices connected without wires. Due to the characteristics of MANET like self-arranging, decentralize and infrastructure less, is prone to security threats A lot of research has been done MANET security but an adequate efficient solution is not found yet. In this paper we propose a new mechanism to detect the attacker using MANET metrics like Hop-count and delay.*

Keywords—*MANET, Wormhole Attack, AODV, Hop-Count.*

1. I. INTRODUCTION

One of the most demanding wireless network is wireless Adhoc network which is also known as IBSS Independent Basic Service Set. It is network where connecting links between devices are wireless and term Adhoc means that each mobile device is doing both jobs i.e., one receving the packet and then forwarding that packet to other mobile nodes. Based on mobile device connectivity, the selection of mobile node that forwards the data is done dynamically [1] .The Adhoc network is categorized into different types based on its applications [2].

1. Mobile Adhoc network
2. Vehicular Adhoc network
3. Smart phone Adhoc network
4. Internet based mobile Adhoc network (iMANET)
5. Militaryand tactical MANET DAVOODHASSAN5@

1.1. Mobile Adhoc Network (MANET)

It is continues self-configuring, infrastructure less and dynamic topology of mobile nodes connected without wires.

1.2. Vehicular Adhoc Network

It is the blind of Adhoc network that allows communications among vehicles and roadside equipments like traffic signals. It allows traffic to operate in a intelligent manure by using artificial intelligence.

1.2. Smart Phone Adhoc Network:

It is the network that makes maxmum use of preexisting hardware (like Bluetooth, WiFi) in market available smart phones to make Peer-to-Peernetwork without depending upon cellular carrier network, wireless access points or traditional network infrastructure.

1.4. Internet Based Mobile Adhoc Network

Here mobile nodes and internet gateway are connected by means of Adhoc network. e.g., CloudRelay.

1.5. Military and Tactical MANET: It is Communication between devices that are used by defense organizations. Here emphasis is on security range.

In MANET [3] mobile nodes have restricted geographical range and sending message to the node that is not in transmission range can be sent through broadcast mechanism. The broadcast mechanism is used by the router for delivery the message to destinations that is not in the sender’s range. The router uses routing protocols for accomplishing the broadcast mechanism. To manage connectivity of very large number of mobile devices that are provide with limited resources like bandwidth, energy and batter backup constraint, is the job of routing protocols. The main obstacle that routing protocols faces are nodes dynamic location i.e., node changes location frequently. The various routing protocols that are used in routng protocols are DSDV(Destination Sequenced Distance Vector) [4], OSPF (Open Shortest Path

First)[5], DSR (Dynamic Source Routing)[6], AODV (Adhoc On-Demand Distance Vector)[7].The main goal of these protocols was to route the packet efficiently, due to which these routing protocols lacks the security measures. There are various security threats to MANET that can create harm to our network like black hole, gray hole, eavesdropping wormhole attack [8].In wormhole attack two far away distinct nodes are connected with high speed tunnel also called wormhole tunnel (Figure1). The node at one end of tunnel attracts packets from the neighbor node by giving offers like lower hop-count; than the normal routes, and passes these packets via tunnel to other end. Where another attacker node delivers into the destination address. Data passing via tunnel may result various data theft attacks like- black hole, gray hole and denial of services (DoS). The rest of paper is categorized into different sections where section II describes related work of wormhole detection, section III provides proposed work and section IV and V provide simulation and conclusion
respectively .

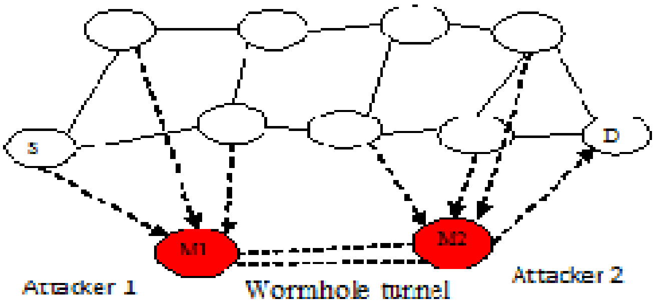

Figure 1. Wormhole attack in MANET

II. LITERATURE REVIEW

L.Hu and D. Evans [9] analyses the wormhole attack and proposed an approach where mobile nodes are outfitted with directional antennas. For the need of communication with each other, nodes use some specialized sector of directional antennas. A relation between the nodes is set if diection of signal between node pair matches. This method is inexpensive and makes best utilization of MANET resources like energy and bandwidth. The only one problem with this approach is that if the attacker puts himself tactically in MANET

Katrin Hoper et.al [10] suggested a protocol that is performing its operation without use of any additional hardware like clock synchronization and directional antennas. In this method routes are discovered first then detection of wormhole takes place by using Hound Packet (uses hop-count as metrics). This approach is very much efficient in detection of large tunnel attacks. This approach is also physical medium independent.

The author [11] proposed a mechanism for detecting wormhole infected path based on determining the Round Trip time (RTT) between two nodes in the network during route discovery phase. The main idea of this approach depends on the fact that the transmission time between the legitimate nodes is lower than the illegitimate nodes. This approach has proven good performance as compared to the rest of techniques and also it does not require any hardware. Although it has minute overhead.

In this paper[12] the author presents a techniques based on clustering by using the digital signature . Here the network is partitioned into different clusters. Each cluster is having a cluster head (CH) and a Gateway for communication with other clusters. For communicating with other clusters the cluster head broadcasts its public key and exchanging of public key of their cluster head is done by gateway. The exchange of data through cluster head and gateway prevents the from wormhole infected path.

III. PROPOSED WORK

We have used Opnet 14.0 Simulator for performing simulation of proposed mechanism. The parameters put under consideration are same as mathematical modeling. The various steps involed in proposed mechanism are given below Figure 2. .Here some assumptions:

N= maximum no of node
X = Randomly Genaerate a number
Tx= Transmitting node(node having same no as value of X)
Dn = Destination node
HC= Hop count of current route
AHC = Average Hop-Count

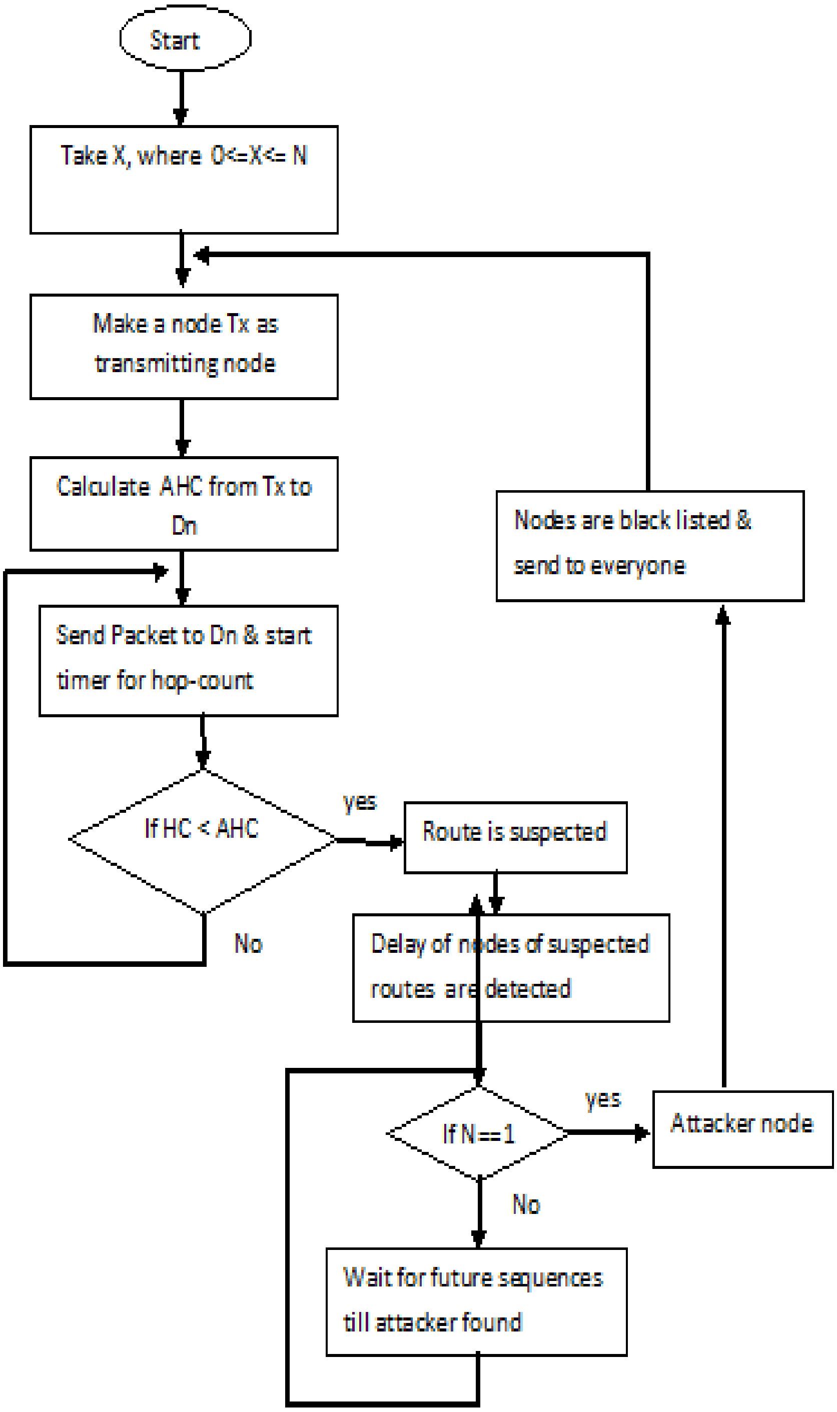
Start
Take X, where 0<=X<= N
Make a node Tx as transmitting node
Calculate AHC from Tx to Dn
Send Packet to Dn & start timer for hop-count
If HC < AHC
yes
No
Route is suspected
Delay of nodes of suspected routes are detected
If N==1
yes
No
Attacker node
Wait for future sequences till attacker found
Nodes are black listed & send to everyone

Figure 2: Wormhole Detection Mechanism

IV. EXPERIMENT RESULT AND ANALYSIS

For performing Simulation we have used following parameters as shown in Fig 3. :

Total no of nodes =50
Infected nodes =6
Packet size =1024 bits
Protocol= DSDV
Packet arrival time =1 sec.
Data Rate = 11Mbps.
Area =20 Sq. Km.

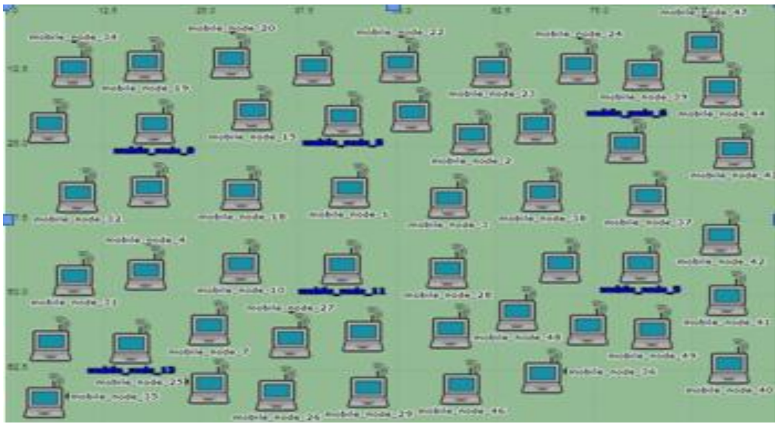

Figure 3: Allocation of nodes with 6 wormhole attacker node.

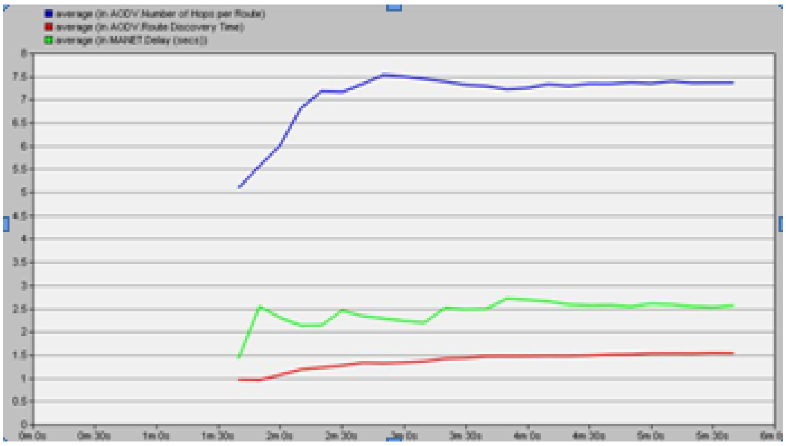

Fig 4: Average Hop-Count of each Path. comparison

As shown in Fig 4. The average Hop-count is reduced 25% by Attacker (Blue Line) from the normal condition (Red Line), the proposed approach recovers the hop-count by bypassing the attacker (Green Line).

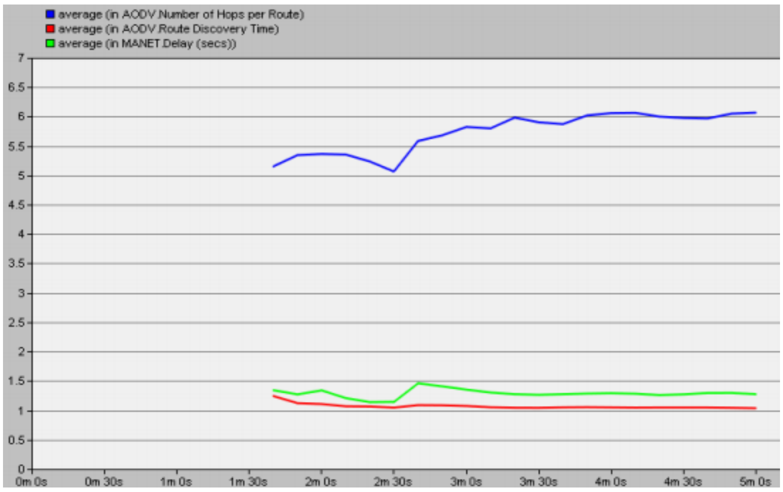

Fig 5: Average Delay of each Path. comparison

As shown in Fig 5. The average Delay is reduced by 75% (Blue Line) from the normal condition(Red Line), the proposed approach have recovered delay by removing attacker (Green).

V. CONCLUSION

In this paper, the proposed methodology for detecting wormhole attack is 75 percent within 5 minutes , here we select some routes from a number of discovered routes for transmission purpose, the probality that routes are reduced in future. This approach also does not use any additional hardware devices like directional antenna, clock synchronization.

In future, we can use large size of nodes , control packet etc for detecting the wormhole attack on large scale.

VI. REFERENCES

[1]. Ozan,k.Tonguy, Gianluigi Ferrari, John Wiley& Sons.ed.Adhoc Wireless Network: A communication Theoretic perspective,2006.

[2]. Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[3]. P.Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc network", In Proc. 6th IFIP Commun and Multimedia Security Conf. ,Sept.2002.

[4]. S.Marti et al., ''Multigatting Routing Misbehaviour in Mobile Adhoc Networks", Proc . 6th Ann. ACM int'l Conf. Mobile Computing and Networking ACM Press, 2000,pp 255-265.

[5]. S. Buchegger and J-Y. le Boudee, "Performance analysis of the CONFIDANT Protocol", In Proc. 3rd ACM Intl, Symp., On Mobile Adhoc Networking and Computing, Jun 2002.

[6]. P.G Argyroudis and D.O' Mahony," Secure Routing for mobile ad hoc networks", IEEE communication Survey and Tutorials, third quarter 2005, vol. 7, no3,2005,258. Authorized licensed use limited to : University of Allahabad. Downoaded on July 30,2010 from IEEE Xplore, Restrictions apply.

[7]. R.Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Performance analysis of Secure Multipath Routing Protocols for Mobile Adhoc Networks, WWIC 2005, LNCS 3510, pp, 269-278, 2005.

[8]. Khabbazian, M.Mercier, H.; Bhargava, V.K Severity Analysis and Countermeasures for the Wormhole Attack in Wireless Network. IEEE Trans. Wireless Commun 2009, 8, 736-745.

[9]. L.Hu and D. Evans, "Using Directional Antenna to prevent Wormhole Attack ", in Network and Distributed System Security Symposium (NDSS), 2004.

[10]. Katrin Hoeper, Guang Gong, "pre-Authentication and Authentication models in Adhoc Network", Signal and Communication techonology, pp. 65-82, 2007.

[11]. Phuong Van et al. "TTM: An Effiecient Mechanism to Detect Wormhole Attack in Wireless Adhoc Networks".

[12]. Dabas , Poonam and Prateek Thakral. " A Novel Technique for the Prevention of Wormhole Attack", International Journal 3, no.6, 2013.