Volume: 05, Issue: 03, Pages:1922-1927 (2013) ISSN : 0975-0290

WPAODV: Wormhole Detection and Prevention Technique

Vikaskumarupadhyay
Department of Computer Science and Engineering, Sagar Institute Of Research And Technology, Bhopal
Email: erupadhyayvikas2010@gmail.com
Rajesh K Shukla
Department of Computer Science and Engineering, Sagar Institute Of Research And Technology, Bhopal
Email: rkumardmh@gmail.com

----------**ABSTRACT**----------
In MANET mobile node is responsible for route establishment using wireless link where each node behave like both as a host and router. MANET encounter by number of security threat because of its open entrusted environment with little security arrangement, whether security over MANET is not to be enhance up to satisfactory level because of its characteristics. Among all of security thread worm hole is consider to be a very serious security thread over MANET. In wormhole two selfish node which is geographically very far away to each other, makes tunnel between each other to hide their actual location and try to believethat they are true neighbours and makes conversation through the wormhole tunnel. Recently research will focus over wormhole detection and prevention but existing technique having lower network overhead lower battery power consumption in order to longer survival of network with fast response. In this paper a dynamic wormhole detection and prevention technique WPAODV has been proposed which is based on an hybrid model that encapsulate location ,neighbour node and hop count method.

Keywords: Adhoc network, wormhole, threshold, AODV

Date of Submission: November 9, 2013 Date of Acceptance: December 26, 2013

I. INTRODUCTION

Wireless network refers to a network, in which all the devices communicate without the use of wired connection. Wireless networks [1] are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network. Mobile ad hoc network is a part of wireless network [2] which is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management. In MANET each node can communicate with the help of its neighbor node that's comes in its radio range each node forward their packet to their neighbor node towards destination where path for transmitting massege packet is suggested by routing protocol as shortest path.

Every routing protocol concentrates over shortest path where some malicious node over network use this greediness of routing protocol and present an illusion of shortest path between two end point of network and attack major traffic over the network.

Wormhole attack attract massage packet and play number of misbehave with that routing packet like scanning of confidential message , drop ,corrupt and change transmitted massage over network.

The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed. In a wormhole 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 [3]. The wormhole 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 [3,4]. 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.

As mentions in above paragraph wormhole attack have a best impact on the network, it must attract a large amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes.

II. SECURITY CONSTRAINTS IN MANET

MANET is vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks [3]. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive or active,

Volume: 05, Issue: 03, Pages:1922-1927 (2013) ISSN : 0975-0290

internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

III. WORM HOLE ATTACK

Wormhole attack is serious threats in MANET, its attack the traffic of network and either scan, change or drops the entire confidential message inside the packet in the time of journey of packet over the wormhole tunnel. As shows in figure 2 in wormhole attack two malicious nodes of different network link together via some physical connection and form a tunnel and present an illusion[9] that node A of network X is neighbor of node B of network Y. Generally wormhole puts theirmalicious nodesat powerful position within the network as compared to other nodes so its attack maximum traffic of network and prevents other routes instead of the wormhole 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 [7].

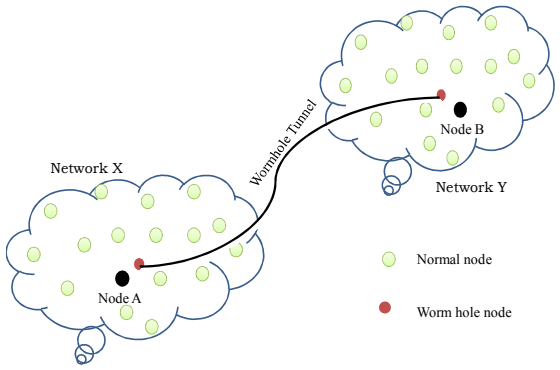

FIGURE : WARM HOLE

I. RELATED WORK

In recent year number of technique has been proposed for the wormhole detection.The proposed work [9] has developed the novel protocol in order to prevent the wormhole attack in the wireless environment. The author has used the symmetric and asymmetric key cryptography with Global positioning system. The protocol has tested on the both GPS node and non –GPS node. The author has tested the protocol with the ratios of GPS nodes to non-GPS nodes 30:20, 25:25, and 20:30, 15:35, 10:40 and 5:45 under a total network area of 100 by 100 meters. This gives the higher results.

The author [10] has proposed the novel approach say RTT-TC that is round trip time measurements and topological comparisons. They have used the AODV routing protocol. First of all the author applies rely on RTT measurements in order to get the suspected wormhole attack and then use the topological comparison approach to real neighbours from the suspected list. Simulation and the results shows that the proposed approach has given a higher detection rate and accuracy of alarms.

The author [11] has proposed a protocol which doesn't uses any special hardware like directional antenna or synchronized clock. This protocol doesn't depend on the physical medium of the wireless network. In this approach the wormhole detection will take place after the discovery of route. Here the hope count techniques have also used between neighbours. The author has also applied the hound packet. The simulation results show that the WHOP is quite excellent in detecting wormhole of large tunnel lengths.

The digital signature is a popular approach to secure the data. In this paper [12] the author has used the Digital signature to defend the wormhole attack. A digital signature has used to verify the sender and the receiver node. Here each legitimate node in the network contains the digital signature of every legitimate node of the same network. Now if the sender wants to send the data then first of all they have to create the secure path. The digital signature will help to create this secure path in the network with the verification. This identification approach will help to find the malicious node from the network. Number of packets, throughput and over head level are compared in this approach which is batter then the previous methods.

The wormhole is a major problem in mobile ad-hoc network. For the best result there are many protocols has developed. The two famous protocols are AODV and DSR. This paper [13] gives the comparison result between these protocols. The parameter considered by the author are: packet delivery fraction, the average end-to-end delay, average jitter, throughput, number of frames tunneled, number of frames intercepted, number of frames dropped, number of frames replayed etc. the results shows that AODV is perfect protocol for the small network. Due to the routing overhead of AODV the performance will decrease in large network. But As the length of colluding link increases, the performancefor DSR degrades compared to AODV.

IV. PROPOSED SOLUTION

This paper presents a mechanism to provide wormhole free path from source to destination by adding an extra feature in AODV routing protocol. Generally AODV routing protocol select a path on the basis of two rule first one is route should be shortest and second one is route should be less traffic.

Proposed scheme add one extra rule over it and now WPAODV avoid the route having wormhole after detection.

In WPAODV proposed scheme used divide and conquer technique over the path suggested by AODV to find whether the route having wormhole or not. For taking decision proposed scheme used Neighbor node concept along with Statistics Based scheme [4] and graphical based solution of wormhole problem.

The main theme of the proposed technique is to discover wormhole in the route suggest by AODV

Volume: 05, Issue: 03, Pages:1922-1927 (2013) ISSN : 0975-0290

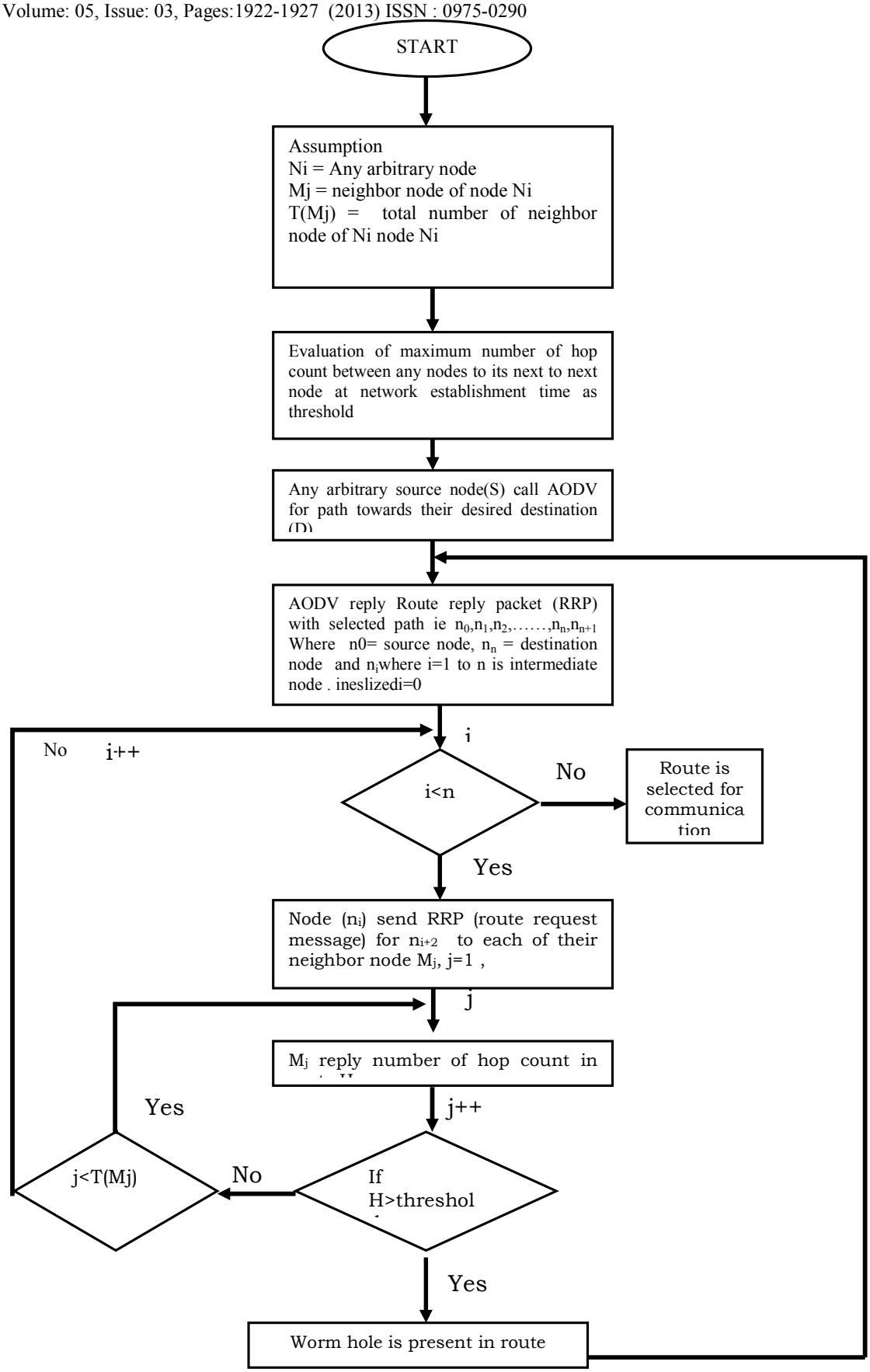

Figure 1:- Wormhole Detection Technique

Volume: 05, Issue: 03, Pages:1922-1927 (2013) ISSN : 0975-0290

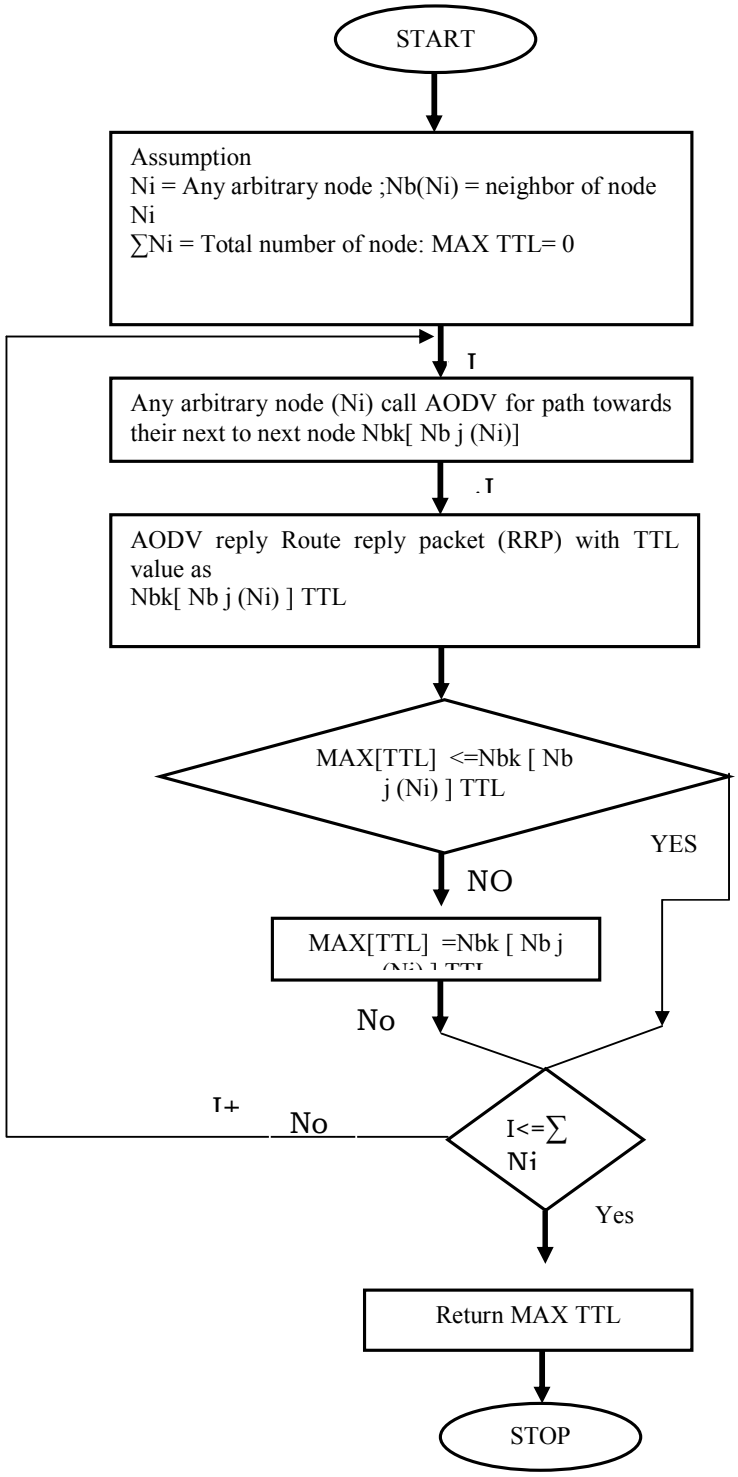

Figure 2:- Max TTL Evaluation

Volume: 05, Issue: 03, Pages:1922-1927 (2013) ISSN : 0975-0290

And this decision will take on the basis maximum number of intermediate node between nodes to its next to next node with alternate route. If alternate route between any pair of node to next to next node with the path discover by AODV is greater than threshold, then it's declared there is wormhole between its next node and next to next node.

Whereas the mechanism for threshold calculation is depend upon hop-count and neighbor node. For calculating threshold each and every node of network find the path having the largest number of node over the entire possible path between it and it's next to next node and consider average value highest hop count of the entire node as threshold over the network as describe in diagram 2.

V. SIMULATION AND RESULT ANALYSIS

In order to authenticate the proposed methodology for wormhole detectionverity of simulation experiments have been performed by using NS-2

For performance validation of proposed technique take different numbers of nodes in each scenario and consider a wormhole tunnels between any two nodes of that scenario for the simulation test.
For experimental verification proposed technique run over three different scenarios with 140,160,180 and 200 node densitieswith same assumptions. As show in figure 1 false negative rate ie rate of wormhole detection is depend network density whereas Threshold that is considered as keyhole for wormhole detection also depends on the network density.

Time Taken to Detect the Wormhole

Wormhole detection is perform by any node in between their next node and next to next node, wither this section describe time required to generate wormhole detection signal by any node successfully.

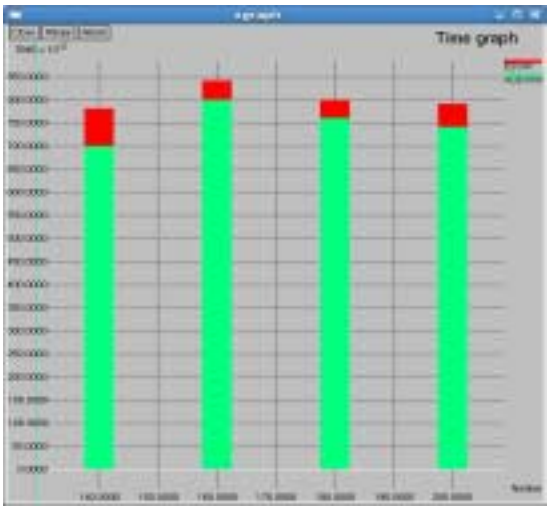

Figure 3Comparison between Proposed method and AODV over time

As show in figure 3 time required to detect wormhole by WPAODV is significantly very less as compare to E2SIW. The averagetime taken to detect a wormhole by the E2SIWis 790 milisecond, whereas it is 560 mili second in the case of WPAODV.

Battery Power Consumption

E2SIW use GPS system for gathering the location of node ie used 1 joule of energy per node to gather it location whereas there is not any requirement of GPS system in WPAODV. One joule energy is 33% of energy used per node in E2SIW so proposed WPAODV degrade the energy requirement by 33%.

Network Overhead

With consider the algorithm 2 for threshold proposed technique is compared with the existing E2SIW in many different factors like network overhead and number for control packet responsible for route hunting and handshaking over different node of network. Proposed technique decrease the possibility of packet retransmission so ultimately decrease the routing overhead as show in figure 4. Along with that proposed technique used number of control packet for wormhole verification over each node so proposed technique having larger number of control packet as compare to AODV.

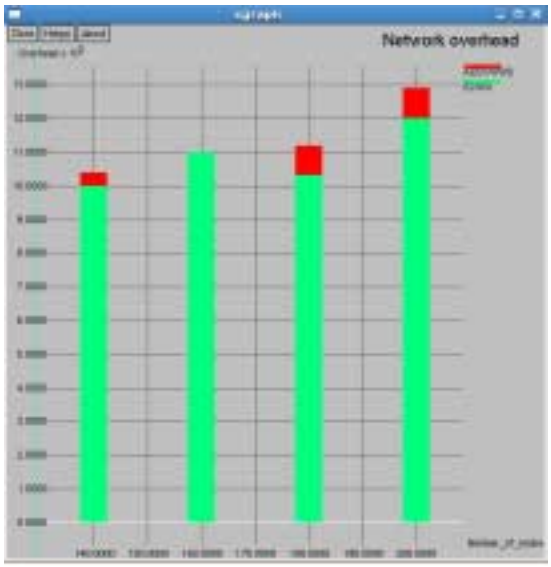

Figure 4Comparison between proposed method and AODV over number of network packet

The above observation shows that the detection technique works efficiently but having some overhead, control packet is also increases in the graph, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol.

Volume: 05, Issue: 03, Pages:1922-1927 (2013) ISSN : 0975-0290

VI. CONCLUSIONS

In this paper a hybrid methodology for detecting wormholes and prevention in mobile ad hoc networks is presented. This method encapsulate advantage of two different predefine method in order to overcome their limitation. The performance of proposed technique is depending upon network density, having lower response time with lower power consumption .

In order to detect wormhole proposed technique use larger number of control packet in future we will try negotiates that effect.

REFERENCES

[1] Maulik, R. ;Chaki, N., "A comprehensive review on wormhole attacks in MANET" IEEE 2010, Page 233-238.

[2] Jian Yin, Sanjay Madria, "A hierarchical secure routing protocol against black hole attack in sensor networks", IEEE SUTC, 2006.

[3] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications" Cambridge University Press 978-0-521-86523-4

[4] Sebastian Terence J , "Secure Route Discovery against Wormhole Attack in Sensor Networks using Mobile Agents", IEEE 2011, pp 110-115.

[5] C. Perkins, E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.

[6] Sang-min Lee, Keecheon Kim "An Effective Path Recovery Mechanism for AODV Using Candidate Node" springerlink, vol. 4331/2006, 2006.

[7] Mahajan, V. ;Natu, M. ; Sethi, A. , "Analysis of wormhole intrusion attacks in MANETS", IEEE 2008, Page 1-7.

[8] Keer, S. ;Suryavanshi, A., "To prevent wormhole attacks using wireless protocol in MANET" IEEE 2010, Page 159-163.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in Proc. of IEEE ICNP, 2002.

[10] Dang QuanNguyen ; Lamont, L., "A Simple and Efficient Detection of Wormhole Attacks", IEEE 2008, Page 1-5.

[11] KatrinHoeper, Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," Signals and Communication Technology, pp. 65-82, 2007.

[12] Kanika Lakhani, Himanibathla, Rajesh Yadav "A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET" IJCSNS International Journal of Computer Science and Network Security, vol. 10 No.5, May 2010.