Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Neighbor Based Efficient Worm Hole Detection and Prevention Technique

[1]Chitra Gupta[*], [2]Brajesh Kumar Shrivash

[1]Department of Computer Science Engg & GITS, India

[2]Department of Computer Science Application& GICTS, India

Abstract— MANET (mobile ad hoc network) is a self organized flexible network. Here wireless devices free to move anywhere in the network. In mobile ad hoc network more security is required then wireless network. The mobile nodes allow communication among the nodes by hop to hop basis and the forward packets to each other. There is no centralized node to control on whole network due to this vulnerability MANET have more security issue, one of them are worm hole attack. In wormhole attacks, packets are tunneled from one malicious node to other malicious node. In our propose work we work on distance ,next_hop, and next to next_hop calculation on this calculation we get whole network scenario and knows about the location of node, so calculate on the basis of location. We detect and prevent worm hole attack.

Keywords— Wormhole attack, AODV, PDR, End to END Delay, Throughput.

I. Introduction

Ad hoc network consists of set of mobile nodes that can be easily added and removed from the network without any centralized administration. It works by broadcasting messages. Nodes participate in routing by forwarding packets to next node till the packet reaches to its destination. Because of their lack of infrastructure and their ability to function without the use of a central authority or Centralized Controlling devices, Mobile Ad-hoc Networks (MANETs) are becoming more and more common. These networks are attractive in those areas where it is expensive to deploy wired infrastructure e.g. disaster areas. A MANET is a collection of mobile nodes where nodes are connected to one another based only upon their mutual understanding. They are nodes without fixed infrastructure and without centralized administration. These nodes are connected via wireless medium, nodes are free to move from one place to another and hence topology is also dynamic. Mobile Ad Hoc Networks [1] are turning out to be more prominent on account of their vital applications extending from health care and logistics, through farming, ranger service, civil and development engineering, to observation and military applications. There are numerous sorts of attacks concentrating on vulnerabilities in routing protocols for mobile Ad Hoc Networks. A standout amongst the most prevalent & genuine attack is wormhole. In wormhole attacks, maybe a couple plotting malicious nodes (wormhole nodes) utilizing a few procedures attempt to draw other honest nodes to send information through wormhole nodes. A short time later, wormhole nodes could misuse the information in assortment of ways: specifically dropping packets to interrupt on correspondence, attempting to break correspondence keys, and so on. Since wormhole nodes don't have to alter or make new packets so no cryptographic procedure can prevent mobile Ad Hoc Networks from wormhole attacks.

II. Worm Hole AttACK

The wormhole attack is an serious attack in mobile ad-hoc network and it's difficult to recognize. For detection of wormhole attack many approach has been proposed. In wormhole attack two mobile node join together, both attacker nodes are placed in strong position of network in two different part of network. By occupying dominant positions in a network these two nodes can cover whole network area and promote to have the shortest path for transferring data. The both attacker nodes are connected to each other using a link which is called wormhole tunnel. The wormhole attack is a serious threat for mobile ad-hoc network that happen in the routing protocol for distracting the user for sending their data and it cannot be detected easily. Its present a illusion of shortest path between two end points in network. For detection of the wormhole attack in MANET a technique has been proposed. 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. 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. Routing protocol over the dynamic link of MANET is responsible to select shortest and less traffic path but it is very challenging because of its mobile nodes and its very tedious job to maintain the accuracy over the network for long time .wormhole attacker node can use that greediness of shortest path, make an tunnel over the network and present an illusion of shortest path via wormhole node. The basic figure [1] of wormhole attack is shown below.

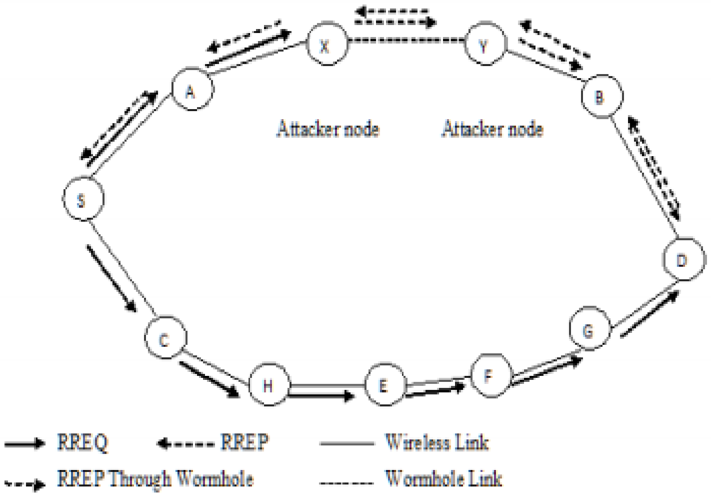

Fig 1: Worm hole Attack [2]

III. TYPES OF WORM HOLE ATTACK[3]

An On the basis of nodes worm hole attacks classified into three parts:

a) Open Wormhole Attack:

The network is available to complete the communication in the network. The two nodes can modify the data and show them self in the way of route discovery.

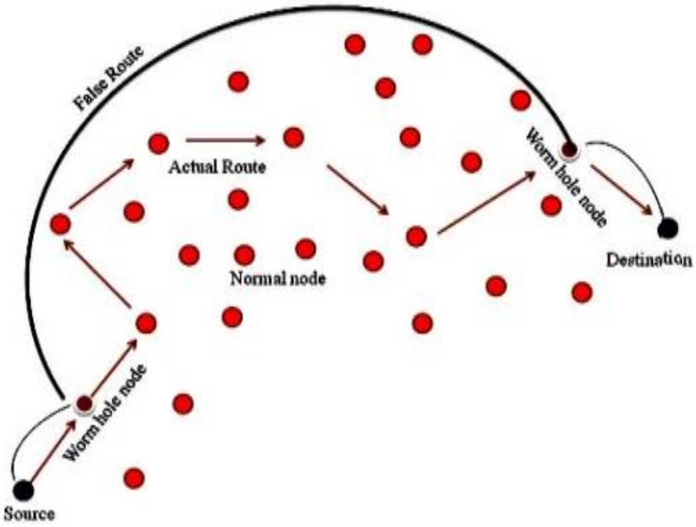

Fig 2: Open Wormhole Attack [3]

b) Half Open Wormhole Attack:

In this type of attack only one node of wormhole malicious node in the network is open to spoil data integrity.

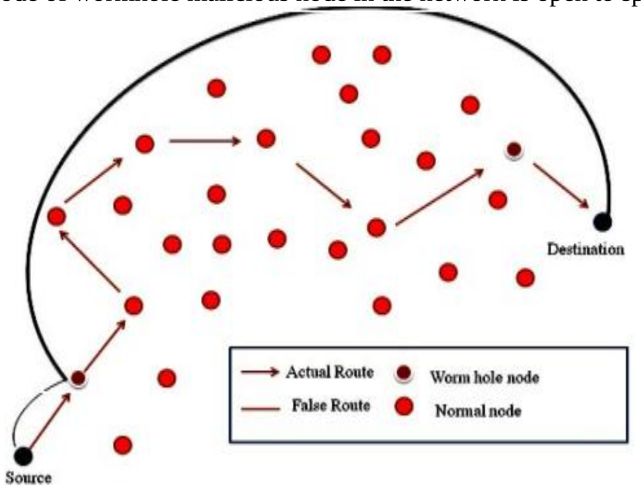

Fig 3: Half Open Wormhole Attack [3]

c) Closed Wormhole Attack:

In closed worm hole attack, when the tunnel has created then both node hide them self from the network but act for modifying the data. They show the shortest path to send the data.

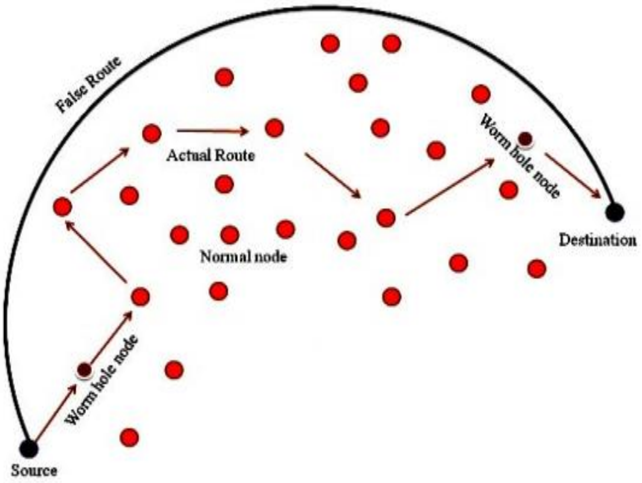

Fig 4: Closed Wormhole Attack [3]

IV. CAUSES OF WORM HOLE ATTACK IN MANET

a) Packet Encapsulation:

In which one malicious node encapsulates the route request and sends it to colliding node which decapsulate it and forwards the route request (RREQ) packet.

b) Out-of-Band:

In Out-of-Band, two malicious nodes sends route request (RREQ) between them by using the long range directional wireless link or direct wired link.

c) High-Power-Transmission:

In high power transmission a malicious node get a route request (RREQ) and broadcast that request with high power level. Any other node that hears the high power broadcast must be a malicious node so it receives that route request and again rebroadcast towards the destination.

d) Packet Relay:

In packet relay two malevolent hubs reply bundle between two hubs which are far separated from one another and convenience these hubs that they are neighbor.

V. AODV PROTOCOL

AODV is a method of discovering route for messages transfer among mobile workstations. It permits these mobile PCs, or hubs, to go messages through most brief way to their neighbors to hubs with which they can't straightforwardly convey. This deciding the courses along which messages can be traded. AODV verifies these courses don't contain circles (loop) and tries to locate the most limited course conceivable. If network has an any error in route establishment AODV can create new route and able to handle changes in route. The networks have many nodes on a wireless network. Each node has limited range of communication. Because of the restricted extent, every hub can just correspond with the hubs by it Nodes you can connect with straightforwardly are thought to be Neighbors. A node spares track of its Neighbors by listening for a HELLO message that every hub telecast at set recesses. At the point when one hub needs to make an impression on another hub that is not its Neighbor it telecasts a RREQ (Route Request) message. The course demand message contains a few key bits of data: the source, the destination, the lifespan of the message and a Sequence Number which helps as an extraordinary ID.

VI. LITERATURE REVIEW

Dimple Saharan et. al. in 2014 proposed a methodology to detect a worm hole attack in manet [5],in this paper they check a effect of worm hole attack is analyzed on AODV routing protocol in MANET and a prevention mechanism is presented to secure the network. A solution is proposed to prevent the network against wormhole attack. For encryption and decryption of hello packets a secret key is used. Because of this only authentic nodes will remain in the network. Worm hole hub (non-legitimate hubs) will be tossed. Accordingly correspondence can occur just between the trusted hubs. So malicious hub (node) can't go into framework and correspondence is secured. In this work they choose AODV as routing protocol for MANET, a pair of wormhole nodes is selected for performing wormhole activity. And simulation is done on NS 2.34 with 36 nodes. Simulation clearly shows that our method is well effective in preventing the network against wormhole attack.

© 2015, IJARCSSE All Rights Reserved

In [2013] Pratima, Ashish, Nitesh at el.[6] The present paper has proposed the hybrid model show to recognize and keep the wormhole attacks. This methodology has been work with neighbor nodes and hop count system. This paper displays a hybrid approach that is in light of hop number and neighbor nodes data plan for wormhole discovery and counteractive action with lower false negative rate and vitality utilization. Spine of Proposed method is assessment of threshold value i.e. most extreme number of halfway nodes between any nodes (N) to node (N+2).

In 2012; Zubair Ahmed, M. Hasan et al[7]. Proposed an enhanced routing table for discovery of suspicious links proposed an updated routing table for recognition of the suspicious connections, affirmation of wormhole presence, toward the end separate the affirmed wormhole nodes. The methodology has been connected to DSDV and the location of independent wormhole nodes and attacks. In this paper they have proposed an approach that will be using the information present in the routing table for the detection of the wormhole links.

Juhi Biswas, Ajay Gupta, Dayashankar Singh et al[8]. Proposed a technique for detect wormhole attack through modified AODV routing protocol. In this research paper work, some modifications have been completed in a wireless ad hoc network direction-finding convention to recognize and evacuate wormhole assault in true MANET. Wormhole assault recognition and avoidance calculation, WADP, has been actualized in changed AODV. Likewise node verification has been utilized to detect malicious hubs (nodes) and evacuate false positive issue that may emerge in WADP calculation. In this paper, they propose an algorithm to detect wormholes without any special hardware's. Our work WADP is an improvement over previously given WAP [3] in a way that WAP suffered from false detection where as WADP is free from false detection when exposed wormhole attack are launched as it consist of detection of malicious nodes through authenticity test and further confirmation of wormhole existence by calculating delay per hop in case of exposed attacks and by neighbor node monitoring in case of hidden attacks. Their mechanism is implemented based on the modified AODV protocol.

In 2012; Pushpendra, Prashant, Rajkumar et al[9]. Proposed a different approach for detecting wormhole using hop count and time delay analysis. The proposed work is simulated using OPNET. Furthermore, since they just select part of the looked routes for multi-path transmission, the likelihood that attacks can possess the routes are further decreased. In another situation, attackers might maliciously alter different nodes rather than itself in the graylist. In this way the nodes that have been altered would be accounted for as modifiers and be obstructed by the source node. To counter this, some ID-based cryptographic techniques [15], for example, signature can be embraced to keep this.

In 2012; Priyanka, H.P. Sinha, Abhay, et al [10] Give a solution for detection and prevention wormhole attack in AODV for mobile ad-hoc network, in this paper, a secret key is utilized for encryption and decryption of hello packets. In view of this, the main real nodes will stay in the network; non-authentic nodes (wormhole nodes) will be disposed of. Accordingly, correspondence can happen just between the trusted nodes. So malicious nodes can't go into framework and communication is secured. In this work AODV is chosen as a routing protocol for MANET, a pair of wormhole nodes is selected for performing wormhole activity. And simulation is done on NS 2.34 with 36 nodes. Simulation clearly shows that, this method is well effective in preventing the network against wormhole attack.

Karthik, K. Vinay in [2012] et.al[11] proposed a method for detection of wormhole attack, In this paper, they have proposed a calculation which distinguishes and remove the wormhole attack in the routing stage itself. their component is in view of the aggregate round trip time (RTT) of the built up route and the normal round trip times of the sender one hop neighbors, which is considered as greatest one hop round trip time. They detect the wormhole link and we avoid the wormhole by blocking that route and selecting another route from the available routes in the routing list. Solution works in both mobile ad hoc networks and wireless ad hoc networks.

VII. PROPOSED ALGORTIHM

```
Step 1: listen of transmit packet $\partial$
Step 2: Take the id of transmit node
Step 3: Calculate the neighbor of node in network and put value in T
Step 4: if(T<n)
4.1 Sparse network
4.2 Every node store value of next_hop and next_next_hop
4.3 Calculate the distance of path node
Step 5: if(T=N)
5.1 Dence network
5.2 Every node store value of next_hop and next_next_hop
5.3 Calculate the distance of path node
Step 6: Send data by shortest path
Step 7: Wait for random tim e(RTT) to get ACK
Step 8: if (Wait>Threshhold)
8.1 Send ENQ_ PACK Neighbors
8.2 Check the information path node in their table.
8.3 Update Their Table
Step 9: Broad cast Enq_packet information to whole Network.
Step 10: put malicious id of node to routing table and mark them.
Step 11: follow next path
```

Enq packet

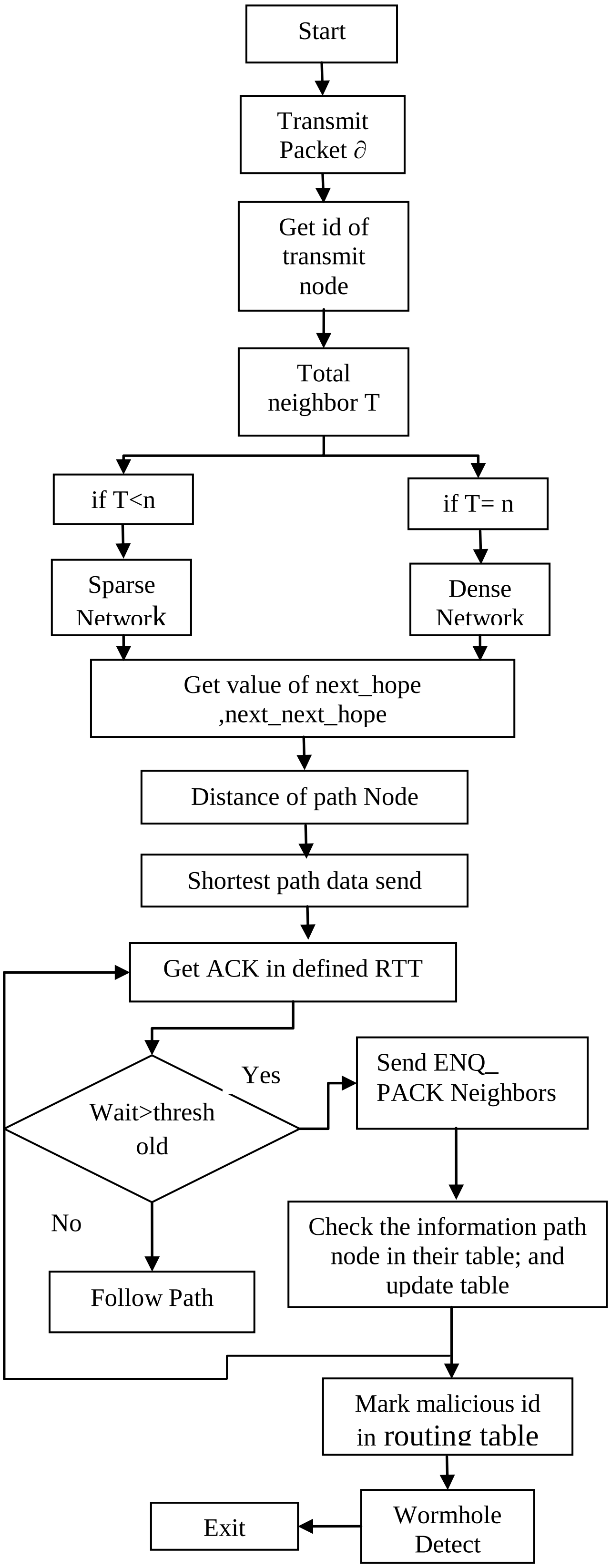

Fig 5: Flow chart of proposed working

VIII. EXPERIMENT RESULT

a) Packet delivery ratio:

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source.

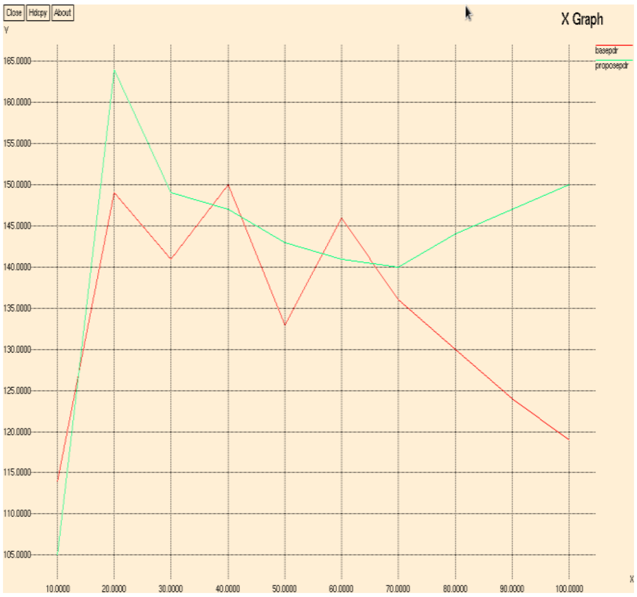

Fig 6: Shows Comparison between base (red) and Proposed (green) values in PDR.

In this graph1 shows when the simulation start minimum packet delivery ratio is 105 and highest is 163 of proposed and the other end base minimum packet delivery ratio is 114 and highest 150. On the basis of comparative results we easily say that our propose work is a novel approach.

b) Throughput:

It is defined as the total number of packets delivered over the total simulation time. The throughput comparison shows that the three algorithms performance margins are very close under traffic load of 50 and 100 nodes in MANET scenario and have large margins when number of nodes increases to 200. Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits received successfully by all destinations.

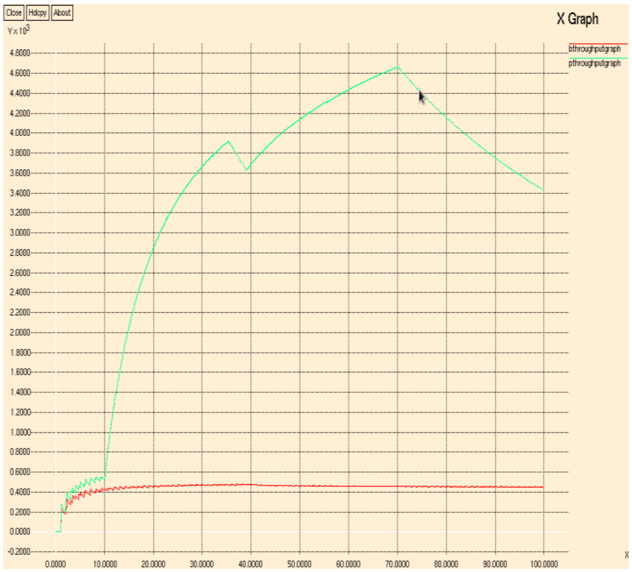

Fig 7: Shows Comparison between base (red) and Proposed (green) values in Throughput.

In graph2 shows the comparison between base and proposed values in throughput. When simulation starts the throughput of proposed work start with 0 and goes to maximum value 470, and the value of base work start with 0.1 and then constantly low. In this way it's not good in real time scenario.

c) Routing overhead:

Routing overhead refers to metadata and network routing information sent by application, which uses a portion of available bandwidth of communications protocols. This additional information, making up the convention headers and application-particular data is alluded to as overhead, since it doesn't add to the substance of the message. Protocol overhead can be expressed as a percentage of non-application bytes (protocol and frame synchronization) divided by the total number of bytes in the message.

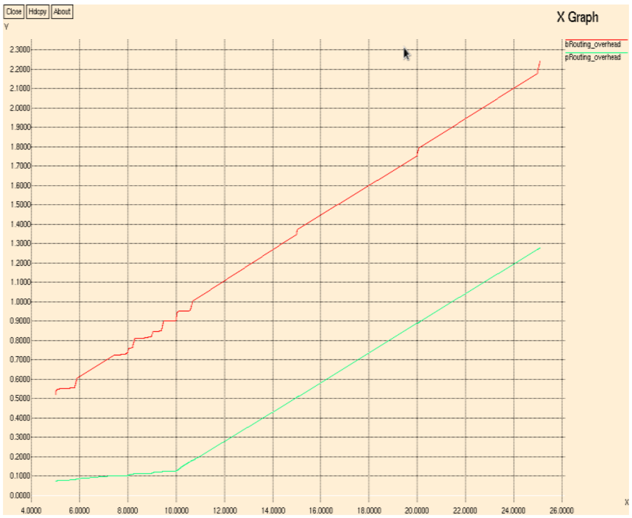

Fig 8: Comparison between base and proposed values in routing overhead.

In graph 3 shows the comparison of routing overhead. When simulation start the proposed value is 0.99 and increased up to 1.29, where as the values of base work is more higher.

d) Send Packet:

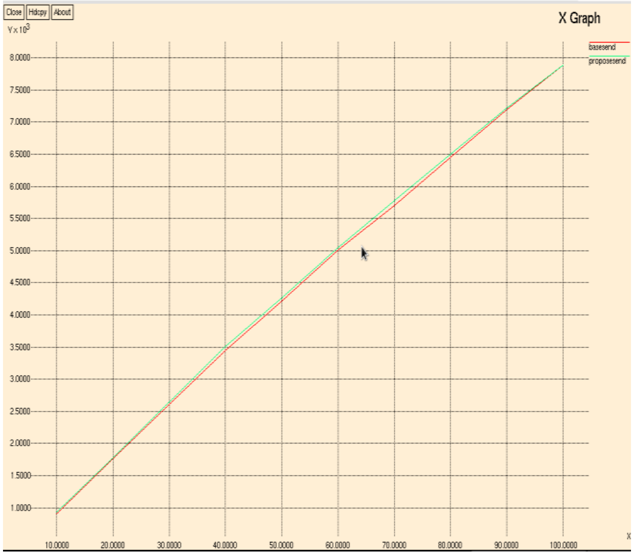

Fig 9: Graph4 Shows Comparison between base (red) and Proposed (green) values in send packet.

In graph 4 shows the comparison of Send packet. When simulation start the proposed value is 0.99 and increased up to 7.80, where as the values of base work is slightly lower down.

e) Drop Packet:

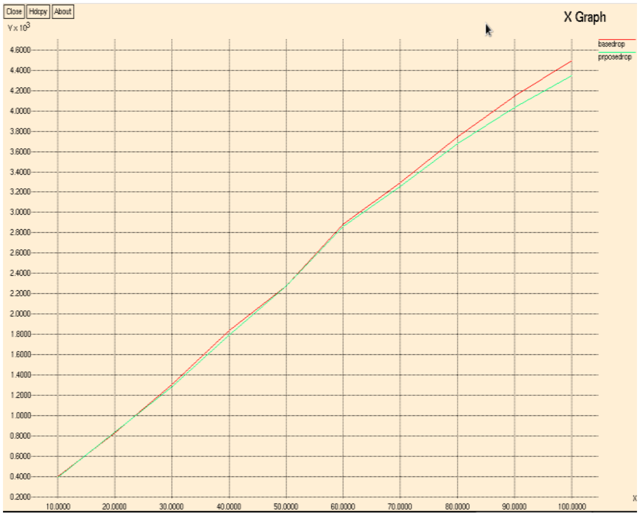

Fig 10: Graph5 Shows Comparison between base (red) and Proposed (green) values in Drop packet.

© 2015, IJARCSSE All Rights Reserved

In graph 5 shows the comparison of Drop packet. When simulation start the proposed value is 0.40 and increased up to 3.95, where as the values of base work is slightly good.

f) Received Packet:

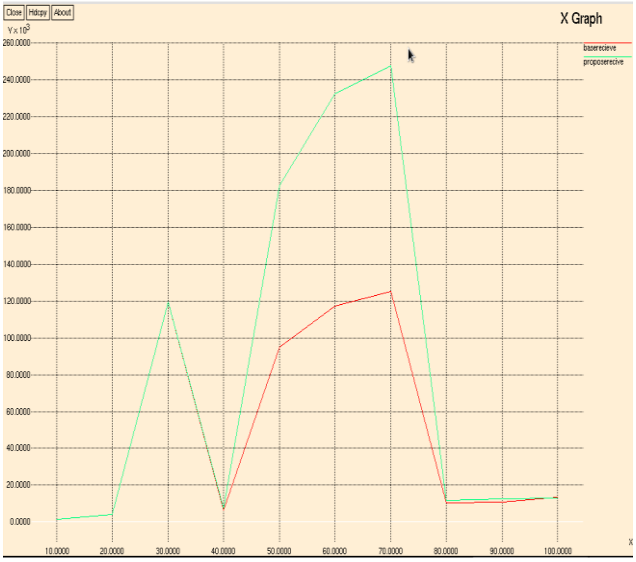

Fig 11: Graph6 Shows Comparison between base (red) and Proposed (green) values in Received packet.

In graph 6 shows the comparison of Recieved packet. When simulation start the proposed value is 0 and increased up to 250, where as the values of base work is not good enough to receive more no. of packet.

IX. CONCLUSIONS

In this paper an efficient method for wormhole attack detection in Mobile Ad Hoc Network is described. The algorithm is implemented in AODV protocol. In this proposed method is provided based on distance, next_hop,and next to next_hop calculation .On the basis of calculation we get whole network scenario and knows about the location of node, so calculate on the basis of location. By this worm hole attack detect and prevented.

REFERENCES

[1] Tran Van, Ngo Trong, HeejoLe "Transmission Time-based Mechanism to Detect Wormhole attacks" ;IEEE Asia-Pacific Services Computing Conference pages 172-178 ,Year2007.

[2] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre "BlackHole and Wormhole Attack in Routing Protocol AODV in MANET" International Journal of Computer Science, Engineer ing and Applications (IJCSEA) Vol.2, No.1, February2012.

[3] Akansha Agrawal, Amit Saxena "Wormhole Detection and Prevention Scheme using Beacon Node Mechanism with Neighbor Node Discovery" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6620-6625.

[4] Anil Kumar Fatehpuria, SandeepRaghuwanshi. "An Efficient Wormhole Prevention in MANET Through Digital signature". International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 3, March 2013).

[5] Dimple Saharan "Detection & Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks (MANETS)" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 9 September2014 Page No. 7979-7985.

[6] Pratima Singh, AshishSrivastava, Nitesh Gupta .A Novel Approach to Detect & Prevent Wormhole Attack over MANET & Sensor n/w towards Lower Battery Power Consumption, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 51-5.

[7] Zubair Ahmed Khan, M. Hasan Islam. "Wormhole Attack: A new detection technique" ,2012.

[8] Zubair Ahmed Khan, M. Hasan Islam. Wormhole Attack: A new detection technique,year2012.

[9] Pushpendra ,Prashant ,rajkumar,rampratap "Detection of Worm hole Attack using Hop-count and Time delay Analysis", ISSN 2250-3153, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012.

[10] Priyanka Sharma, H.P. Sinha, AbhayBindal. Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks, International Journal of Computer Applications (0975 – 8887) Volume 95– No. 13, pages 34-38,June 2014.

[11] Priyanka Sharma, H.P. Sinha, AbhayBindal. Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks, International Journal of Computer Applications (0975 – 8887) Volume 95– No. 13, pages 34-38,June 2014.

© 2015, IJARCSSE All Rights Reserved