ISSN XXXX XXXX © 2017 IJESC

IJESC

Research Article Volume 7 Issue No.11

To Mitigate Wormhole Attack by using Trusted AODV with WAP - TSH methodology for MANET

Prof. Dr. M. Narayana[1], L.Bhavani Annapurna[2], K.Varalaxmi[3]
HOD[1], Associate Professor[2], M.Tech Scholar[3]
Department of ECE
JayaPrakash Narayana College of Engineering, Ahabubnagar, Telangana, India

Abstract:
Wireless network is a mobile ad-hoc network (MANET) that means nodes are move dynamically in network. In network layer there be lot of attack but introduce only wormhole attack. When more than one malicious nodes are create tunnel is called wormhole attack. In this project we using trusted AODV routing protocol which trust value calculate using tangent hyperbolic function. But here based on trust calculation some delay time should be high at some level of transmission time. We propose a new fresh wormhole detection and prevention algorithm will effectively notice the wormhole attack in mobile ad hoc network. The result shows performance improvement as compared to Trusted AODV protocol.

Keywords: MANET, AODV, worm hole attack, trusted AODV, NS2.

1. INTRODUCTION

A mobile ad-hoc network (MANET) is wireless network that means it's not recurred infrastructure. In MANET nodes are move energetically nature. The dynamic natures of MANET make it more vulnerable [1]. In network layer many attacks possible but we focus only worm hole attack. When more than one malicious node are create tunnel is called wormhole attack [2]. Due to high mobility of mode routing is big challenge in ad-hoc network. In the proposed work, trust based routing protocol is defined in which trust computation is done using tangent hyperbolic function which calculate the trust value of their neighboring nodes promiscuously.

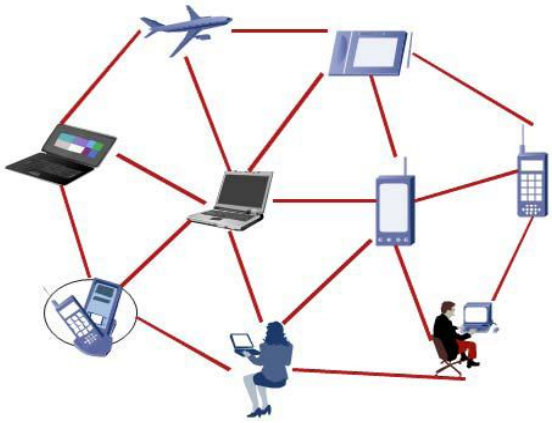

Figure.1. Mobile ad hoc network architecture

In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations.

1.1 AODV routing protocol:

AODV routing protocol is work on ad hoc network. Its use three parameter first RREQ message which request wide-ranging transmit to every neighbor nodes, second RREQ message which use unicast technique during communication and RERR Route error. Mostly AODV routing protocol routing progression necessity is base on sequence number. This is removing the difficulty of calculation in the direction of infinity. In fig.2 display the REEQ and RREP message exchange between S & D [4][5].

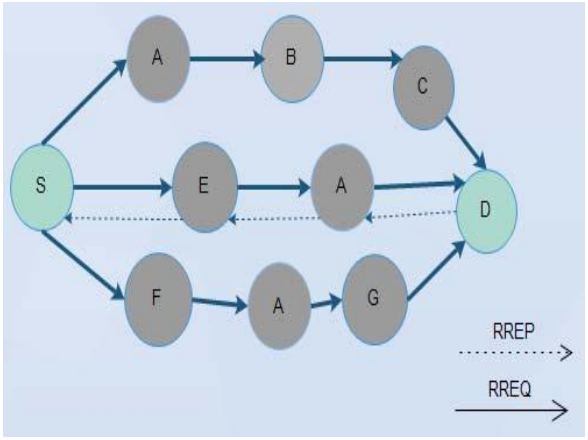

Figure.2. RREQ and RREP message exchange between S& D

1.2 Wormhole attack:

Two malicious node is create a tunnel is called worm hole attack. Means two join together nodes that are far apart are linked by a tunnel giving am is apprehension that they are

neighbors. each one of these nodes allow route request and topology manage communication from the network and send it to the other collude node via tunnel which determination then replay it interested in the network starting there. Through by this extra tunnel, these nodes are able to advertise that they have the direct path through them. just the once this link is establish, the attackers may choose each other as multipoint relays, which then lead to an replace of various topology manage messages and data packets through the wormhole tunnel and Worm hole node drop all the packets[4,5].

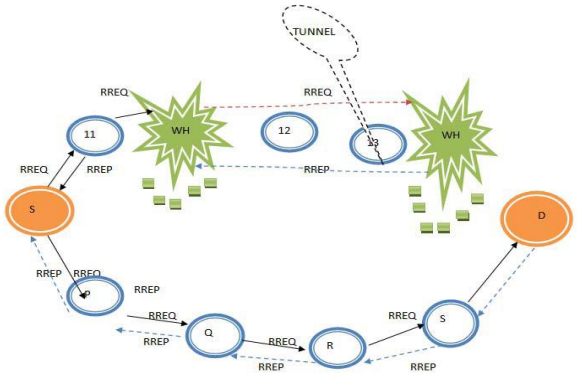

Figure.3. wormhole attack

1.3 TRUSTED AODV routing:

Trusted AODV is a trusted routing protocol based on trust model for mobile Ad-hoc network. Trusted AODV has many relevant features like Nodes perform trusted routing behaviors mainly according to the trust relations between them .A node that performs malicious behaviors will finally be detected and denied to the entire network. System routine is improved at every routing hop[5].

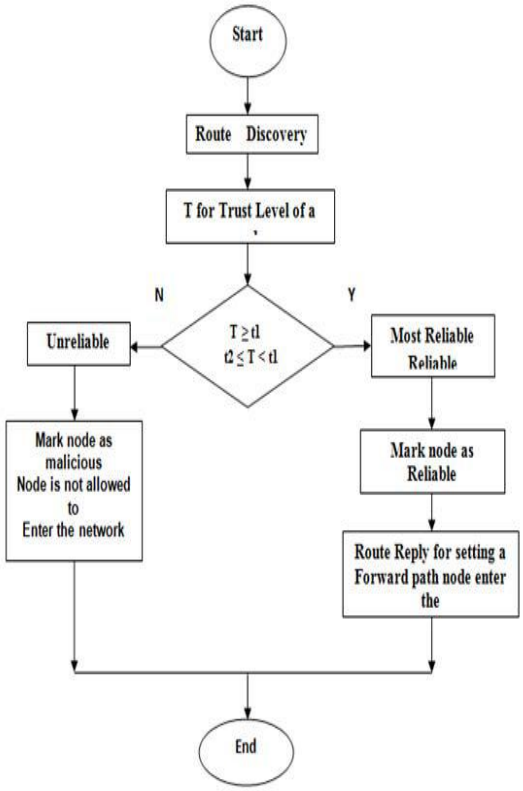

Figure.4. Flowchart for TRUSTED AODV MODEL

1.4 Trust category of a node:

In this work the AODV routing protocol is embedded along with the trust function. The communication between the nodes in the mobile Ad-hoc network depends on the cooperation and the trust level with its neighbors. Based on the trust on neighbor and appropriate threshold values the nodes be capable of be categorize in to the subsequent.

I. Unreliable: it's having trust value between 0 to 0.5.
II. Reliable: it's having trust value between 0.4 to 0.7.
III. Most Reliable: it's having trust value between 0.7 to 1.

During the route discovery phase of the AODV Routing protocol, the trust value is also computed for Everyone the neighbors of some node. The result of trust estimation function is the Trust-status of each and every one of neighbors as Most Reliable, Reliable or Unreliable.

1.6 Threshold value of a node:

Different threshold values are defined for different type of neighbors to develop into Most Reliable, Reliable and Unreliable. **T***ur*, **T***r* and **T***mr* are the threshold values for the Unreliable, Reliable and the Most Reliable respectively[5].

We evaluate a Trust estimation function for the calculation of trust value.

T = tanh (R1+R2) **(1)**

Where **tanh** is tangent hyperbolic function, which has value

tanh x = (ex - e-x)/(ex + e-x) **(2)**

T= Trust value

R1= percentage between the number of packets really forward and number of packets to be forward.

R2= percentage of number of packets received from a node but originate as of others to total number of packets acknowledged from it. After evaluation Trust value is -1 to +1, but use our propose solution value between 0 to +1.

2. METHODOLOGY:

2.1 Algorithm:

Step1: whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcasts RREQ packets through neighboring nodes. RREQ packet contains destination address and sequence number along with source address. Sequence number provides the freshness of the route.

Step2: once an RREQ packet is received by an intermediate node and verifies destination address. If the destination address not matches with the RREQ packet then forwards it to its next hop. This process is repeated until it reaches the final destination.

Step3: route path nodes are saved in routing table.

Step4: when source node starts sending packets, it sends to next node and that node sends to next until it reaches destination. The traversed path nodes are checked with the path nodes in routing table.

Step5: if the traversed path nodes are not in the routing table, wormhole is detected and it is out band wormhole.

Step6: while sending packets to next neighbor node, PDR is calculated for each node. The ratio of sent packets to received packets is calculated for each node.

Step7: Hello packets also sending to each node along with packets until it reaches destination. Roundtrip time is calculated for each consecutive node. if the roundtrip time is less than threshold, that link is high speed link and the two nodes are malicious and detected as wormhole. And also if the PDR is less than 1, that node is wormhole node. The wormhole detected is active wormhole as it affects the packets.

Step8: If PDR less than 1 and RTT are not less than threshold means the loss may be due to traffic.

Step9: If PDR not less than 1, check for RTT less than threshold or not. If it is less passive wormhole is detected as the packets are not affected. If it is not less than the threshold, there is no wormhole.

Step10: Wormhole nodes are announced to all other nodes. All nodes remove wormhole node id from its neighbor table and routing table. If any forwarding node receives the wormhole announcement node, it will send RREP message to source. It will reinitiate route discovery process, and find the new path to the destination without wormhole node.

(a)Hardware Requirements:

System: Pentium IV 2.4 GHz.
Hard Disk: 50 GB.
Floppy Drive: 1.44 Mb.
Monitor: 18 VGA Color.
Mouse: Logitech.
Ram: 2048 Mb.

(b) Software Requirements:

Operating system: Ubuntu 14.04/linux mint/red hat linux 9
Coding Language: otcl, c++ Tool: Ns-2.35

3. RESULT ANALYSIS

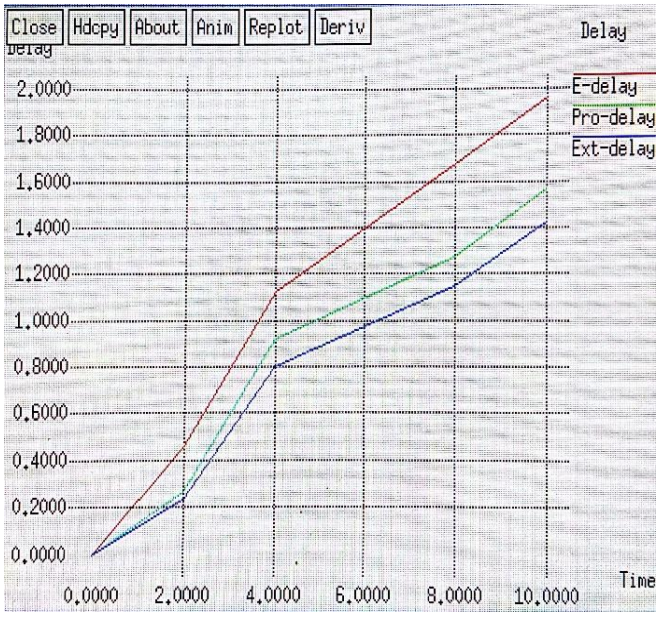

Figure.5. Delay v/s Time

Delay:

In this Graph shows and represents end 2end delay and it shows a simulation time versus delay. The Performance of algorithm improves delay it means decrease the delay compare to existing Trusted AODV routing.

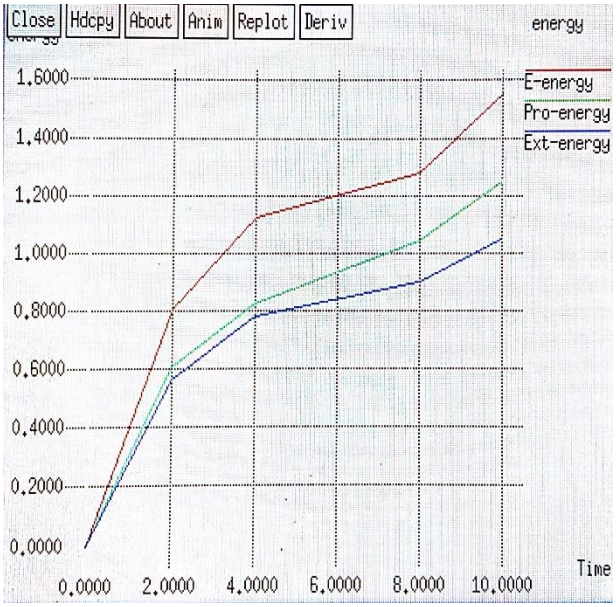

Figure.6. Energy v/s Time

Energy:

In this Graph shows and represents energy consumption and it shows a simulation time versus energy. The Performance of algorithm improves energy values compare to existing Trusted AODV routing.

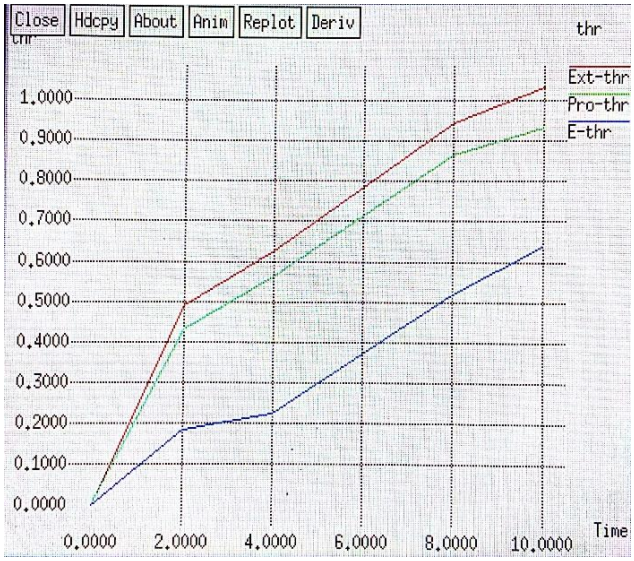

Figure.7. Throughput v/s Time

Throughput:

In this Graph shows and represents throughput and it shows a simulation time versus throughput. The Performance of algorithm improves throughput compare to existing Trusted AODV routing.

4. CONCLUSION:

In this paper, we focused on detection and removal of wormhole attack during data transmission. The proposed algorithm provides more security to ad hoc networks and also prevent from such kind of attacks. It helps to increases the packet delivery ratio and reduces the control overhead by improving the performance of the routing protocol. Here we are discovery

following conclusion on NS-2simulation. Like End to end delay of new fresh algorithm is better compare to TAODV. In future, we also plan to improve the table entries at destination node to get the detection of wormhole nodes faster. And also improve the security of wireless ad hoc networks. By deploying such efficient methods to prevent DoS attacks and hybrid attacks with the help of new fresh algorithm.

5. REFERENCES:

[1]. A Sharma, D bhuriya, U singh, "Secure data transmission on MANET by hybrid cryptography technique", IEEE 2015 International Conference on Computer, Communication and Control (IC4), 10-12 Sept. 2015 Pages1 – 5.

[2]. Jin-Hee Cho, Kevin S. Chan, Ing-Ray Chen et al., "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks", ACM 28th Symposium on Applied Computing, 2013 Pages 1949-1956.

[3]. Reshmi Maulik and Nabendu Chaki "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pages. 271-279.

[4]. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003pages 1 -11.

[5]. Isaac Woungang, Sanjay Kumar Dhurandher, Mohammad S. Obaidat, Issa Traore et al.," Timed and Secured Monitoring Implementation against Wormhole Attack in AODV-Based Mobile Ad Hoc Networks", IEEE, May 2013 pages 1-5.

[6]. Mohammad Rafiqul Alam, King Sun Chan et al.," RTT-TC: Topological Comparison Based Method to Detect Wormhole Attacks in MANET", Communication Technology (ICCT), 2010 12th IEEE International Conference on Nanjing IEEE, 2010 pages991 – 994.

[7]. Soo Young Shin, Eddy Hartono Halim eet al., "Wormhole Attack Detection in MANETs using Route Redundancy and Time based Hop Calculation", ICT Convergence (ICTC), 2012 International Conference on Jeju Island IEEE, 2012. Pages 781 –786.

[8]. Naveen Kumar Gupta, Kavita Pandey et al., "Trust Based Adhoc on Demand Routing Protocol for MANET", Contemporary Computing (IC3), 2013 Sixth International Conference on Noida IEEE, 2013 pages 225-231.

[9]. Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In IEEE WCNC 2005, Seattle, WA, USA, 2005; pp. 1193–1199.

[10]. Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In Dependable Systems and Networks (DSN), pages 612–621, Jun 2005.