ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Detection of Wormhole Attack using Trust based T-Aomdv Protocol

Seema B.P, Roopa Banakar

M. Tech student, Department of CSE, Sapthagiri College of Engineering, Bangalore, India

Assistant Professor, Department of CSE, Sapthagiri College of Engineering, Bangalore, India

ABSTRACT: the nodes in MANETs dynamically change their topology and for this reason require an efficient mechanism for data transmission. MANET is inclined to a number of form of attack such as black gap, wormhole, Sybil, flooding attack, grey hole. The Wormhole attack is among the more suitable energetic attacks that are elaborate; two colluding malicious nodes create a tunnel between them using a private high speed network(s). This attack allows a node to short-circuit the normal flow of routing message. The attacker at one end collects the data and replays them at the other end .in this paper we have used T-AOMDV, Maximum HopCount(MHC) and AES based Encryption for detection of Wormhole attack.

KEYWORDS: MANET, T-AOMDV, MHC, AES.

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. Two nodes out of direct communication range need intermediate nodes to forward their messages. Due to multi-hop routing and open working environment, MANETs are vulnerable to attacks by selfish or malicious nodes, such as packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. The most target area of research in mobile ad hoc networks is to provide a trusted environment and secure communication. There are several applications of ad hoc network which need highly protected communication. Common applications of MANET are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation such as after natural disaster like a flood, tornado, hurricane and earthquakes

The AOMDV routing protocol is a multipath extension of the AODV protocol which aims to find loop-free and link-disjoint multi paths during route discovery. AOMDV uses advertised hop-count to guarantee loop free feature. AOMDV route tables have a list of paths for each destination to support multipath routing. All paths to a destination have same destination sequence number. AOMDV route maintenance is similar to that in AODV. A RERR for a destination is generated when last path to that destination fails. The basis of the AOMDV protocol is in guaranteeing that multiple routes revealed are loop-free and disjoint, and in discovering paths through a flood-based route discovery. AOMDV path revise rules exploited locally at every node and have a major role in preserving loop-freedom and disjoint-ness characteristics.

Wormholes are classified based on resources used for attacks:

1. According to attack mode, Wormhole isclassified as:
    a) Wormhole using encapsulation
    b) Wormhole Out-of-Band Channel
    c) Wormhole with High Power Transmission
    d) Wormhole using Packet Relay
    e) Wormhole using Protocol Deviations

2. Depending on whether attackers are visible in paths Wormholes are classified as:
    a) Open Wormhole Attack:

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

The attackers are themselves in a RREQ packet header following route discovery procedure. Other nodes know that malicious nodes lie on the path but think that such nodes are direct neighbors.

b) Half open Wormhole Attack:
One side of a wormhole does not modify a packet and only the other modifies the packet after route discovery procedure.

c) Closed Wormhole Attack:
The attackers do not modify packet content, even when the latter s a route discovery packet. Instead they simply tunnel the packet from one side of the wormhole to the other and rebroadcast the packet.

3. Depending on resources used for an attack Wormhole is classified as:

a) Out-of-band wormholes: The colluder nodes establish a direct link between a wormhole tunnel's two end-points in a network. This link is created using an external wired link. This is also called Hidden Wormhole Attack, using hardware introduced by attacker and without compromising network hosts.

b) In-band wormholes: An in-band wormhole needs no additional hardware infrastructure. It consumes existing communication medium capacity to route tunneled traffic. Thus, the network's own nodes are involved in the attack. This attack is of 2 types: self-contained in-band wormhole and extended in-band wormhole.

c) Self-contained in-band Wormhole: a subtype of "Inband wormhole" it uses network resources and involves other nodes in the network. Intruders create a false linkbetween attacker nodes themselves.

d) Extended in-band Wormhole: Also known as Exposed Wormhole Attack and Byzantine Wormhole Attack , it is another "In-band Wormhole" subtype which creates awormhole that extends beyond attackers by
Forming tunnel endpoints. A false link is advertised between two nodes which are not attacker nodes
.

II. RELATED WORK

ZolidahKasiran et al [2] study the wormhole attack in mobile ad hoc networks and in order to simulate the impact implements a simulation. According to their description the Mobile Ad hoc Networks is a collection of wireless devices that communicate by dispatching packets to one another or on behalf ofanother device or node, whilehaving not any central network authority or infrastructure controlling data routing. In order to communicate oneanother, the nodes cooperatively forward data packets to differentnodes within the network by using the routing protocol. The simulation result has shown that there is difference performance in throughput when there is an attack.

Thi Ngoc Diep Pham et.al [3] propos statistical approach using infrastructure nodes to notice the presence of the wormhole and localize the wormhole endpoints placement. The simulation results demonstrate that their mechanism is simpler than the related method called prohibited topology technique, especially in high-speed network such as vehicular DTN.

FreekVerbeek et.al [4] propose an algorithm that mechanically proves routing functions deadlock-free or outputs a minimal counter-example explaining the source of the deadlock. Their algorithm is the first to automatically check a necessary and sufficient condition for deadlock-free routing.

Isaac Woungang et al [1], a secured AODV-based routing theme (TSMI) are planned for mitigating such attacks. Simulation results are provided to demonstrate the effectiveness of their approach, using the packet delivery ratio, the number of broken links detected and numberof packets received by destination, as performance indicators

III. PROPOSED SYSTEM

Figure1 Shows the Architecture of our proposed system.It includes following modules:

a. *Network Initialization*

Network initialization is to specify various network parameters before actually starting a network. The parameters include the working channel, the network identifier, and network address allocation.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

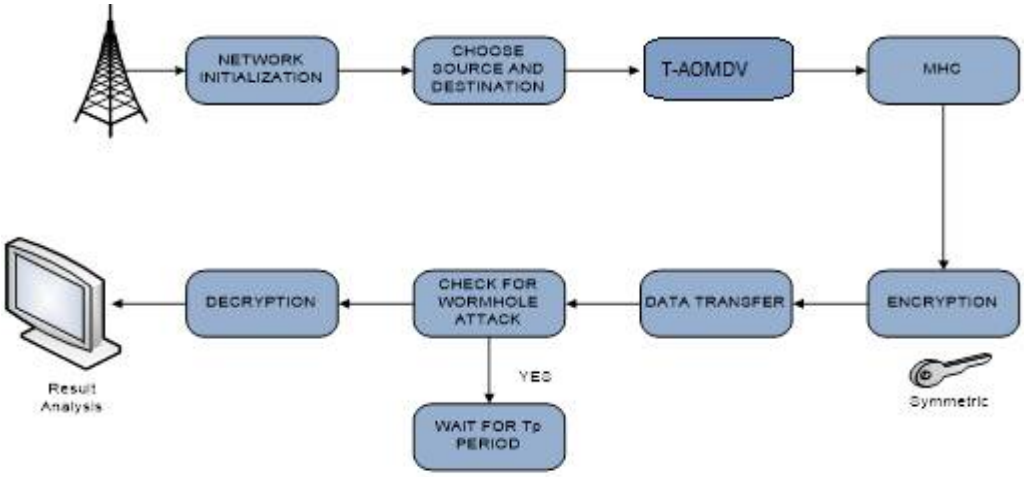

Figure 1: Proposed Architecture

b. Choose the source and destination:

Users will enter the source and destination nodes for data transmission.

c. T-AOMDV

The AOMDV protocol locates multiple paths involving two stages which are:

i) A route update rule establishes and maintains multiple loop-free paths at every node, and

ii) ii) A distributed protocol locates link-disjoint paths.

AOMDV protocol locates node-disjoint or link disjoint and it is dependent more on routing information previously available in the fundamental AODV protocol, thus preventing overhead acquired to determine multiple paths. Specifically, it does not use any specific control packet. Additional RREPs and RERRs for multipath discovery and protection together with extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) are the only extra overhead in AOMDV compared to AODV. AOMDV suppresses duplicate Route Requests (RREQs) at intermediate nodes in two different variations, resulting in either node.

AOMDV can be configured to either to discover the link or node disjoints paths. Disjoint alternate paths are a better choice than overlapping alternate paths, as probability of interrelated and concurrent failure is reduced. This helps in an adversarial environment where malicious activity can lead to additional link failure. Finding a disjoint path is straightforward in source routing, but hop-by-hop routing i.e. AOMDV is more efficient regarding creating less overhead number of paths in any source and destination and is directly proportional to number of nodes in the network. AOMDV worksefficiently in dense and heavy networks.

d. MHC (maximum hop count value)

In proposed methodology every hops over the route responsible to find out, is there any worm hole between its next hop to its next to next hop over the rout? For detection every hop evaluate an alternate route for their next to next hop over the route and if number of hop count in any of alternate route is greater than MHC(maximum hop count value) than that node reply wormhole detection signal between its next hop and its next to next hop and discard that path .MHC means maximum number of hop count with any alternate route between any nodes to its neighbor of neighbor nodes ie any nodes to its second stage node .For calculating MHC each and every node of network find the largest number of hop count required for its next to next node with any alternate route over the network. And consider average of it's as MHC value

Algorithm for MHC

HC=Hop count

MHC=Maximum hop count

Algo:-

For

(I=1; I

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

<=N ; I++)
{
For (J=1; J<=X ; J++){
Step 1. Si send an route request message to all its
neighbor node for its next to next node NNjSi
Step 2. All the neighbor node reply the Route through
route Reply packet to Si in term of number of hop count 'Y'
Step 3.if (Y>HC)
HC=Y
}MHC= MHC+ HC
}MHC = MHC/N

e. Encryption using AES:

The design of AES encryption module is implemented on a chip of FPGA. Round-key generation and round operation adopt the mode of parallel computation and it can support three kinds of key length such as 128, 192 and 256 bit. The proposed scheme has the following properties: A temporary storage is used for the round operation. The processor performs each round operation while the round-key of the next round is generated. So, round-Key requires no extra storage. In this way, it not only saves the on-chip resources but also solves the delay problem caused by reading the key and it improves the clock frequency and the throughput of the system and reduced the memory requirements of the round key.

After encryption data is transferred to network, at each node there is a check for wormhole attack if present need to wait for a period of time to resend the data, when data reaches its destination it is decrypted using AES.

VII. RESULTS

In this section we have computed performance analysis using different parameters:

1. *Delay:*

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and data packet transmission. Only the data packets that successfully delivered to destinations that counted. The lower value of end to end delay means the better performance of the protocol. Graph 2 describes end-to-end delay our proposed system.It is calculated using:

$$\sum(arrivetime - sendtime) / \sum Numberofconnections. \quad (1)$$

2. Packet delivery ratio

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

$$PDR = S1 \div S2 \quad (2)$$

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. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes

Below graphs shows the comparison between the existing systems to proposed system. A plot of graph for different values of end to end delay vs no.of.nodes is as shown in the Figure2. Delay of packet receiving at the receiver side is less compared to existing methods. In figure 3 plots the values of packet delivery ratio vs no.of.nodes.as the communication increases that is transmission of rate of packets increases delivery rate is also high in our proposed system.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

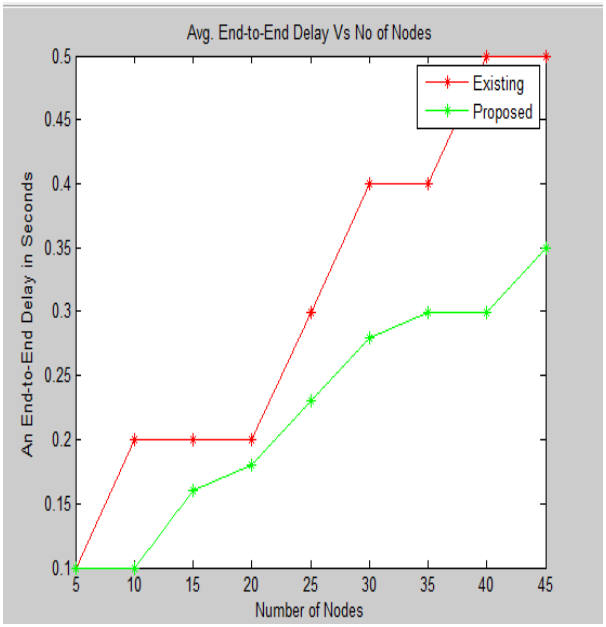

Figure2:shows the graph for end to end delay Vs. No of Nodes.

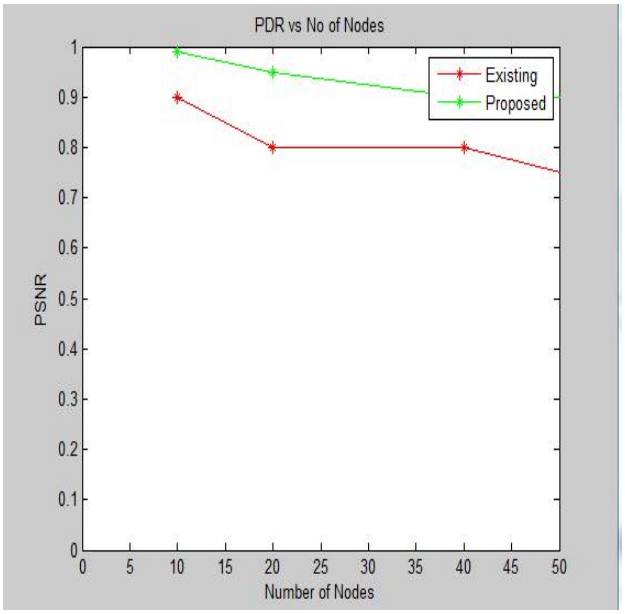

Figure 3:shows the graph for PDR Vs. No of Nodes.

VIII. CONCLUSION

The wormhole attack is a type of attack that performs the malicious activity by creating own link and avoids actual link i.e. the actual path for data delivery. The overall idea of this system is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. This protection scheme provides the protection against wormhole attack and blocks the activities of attacker node. Performance analysis shows our proposed method is more accurate than the existing methods.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

REFERENCES

[1]. Isaac Woungang, Sanjay Kumar Dhurandher,IssaTraore, Mohammad S. Obaidat, "A Timed and Secured Monitoring Implementation Against Wormhole Attacks in AODV-Based Mobile Ad Hoc Networks", International Conference on Computer, Information and Telecommunication Systems (CITS), Vol.3, No.2,pp.1234-1245,2013.
[2]. Zolidah Kasiran and Juliza Mohamad, "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", IEEE,pp.23-45,2014.
[3]. Thi Ngoc Diep Pham, Chai Kiat Yeo, "Statistical Wormhole Detection and Localization in Delay Tolerant Networks", the 11th Annual IEEE CCNC -Security, Privacy and Content, No.12,pp-456-478,2014.
[4]. Freek Verbeek and Julien Schmaltz, "A Decision Procedure for Deadlock-Free Routing in Wormhole Networks", ieee transactions on parallel and distributed systems, Vol. 25, No. 8, 2014.
[5]. Ahmed Louazani ,Larbi Sekhri,BouabdellahKechar, "A Time Petri Net model for Wormhole Attack Detection in Wireless Sensor Networks", International Conference on Smart Communications in Network Technologies,2013.
[6]. M. S. Obaidat, I. Woungang, S. Dhurandher, and V. Koo,"Preventing packet dropping and message tampering attacks on aodv-based mobile ad hoc network," in Proc. of the IEEE Intl. Conference on Computer, Information and Telecom. Systems, Amman, Jordan. 2014.
[7]. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, 2012.
[8]. Saurabh Gupta, Subrat Kar and S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", International Conference on Innovations in Information Technology,2011.
[9]. Vikas Solomon Abel, "Survey of Attacks on Mobile Ad hoc Wireless Networks", IEEE,Vol. 3 No. 2,2011.
[10]. Rashid Hafeez Khokhar, MdAsriNgadi, Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", 2008 International Journal of Computer Science and Security. Vol. 2, No.3.