DEFENDING WORMHOLE ATTACK IN MANET

R.Rasathi[1], R.Sumathi[2],B.Anantharaj[3]

[1,2] Final Year B.E CSE students,[3] Head of the Department CSE,
Thiruvalluvar College of Engineering & Technology, Vandavasi, TamilNadu
raviram28198@gmail.com[1],
nilaselviramadass@gmail.com[2],ananthu_arun72@yahoo.com[3]

ABSTRACT -A wireless ad hoc network (WANET) or MANET is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks .A mobile ad hoc network, also known as wireless ad hoc network or ad hoc wireless network, is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly**.**MANETS over networks with a fixed topology include flexibility (an ad hoc network can be created anywhere with mobile devices), scalability (you can easily add more nodes to the network) and lower administration costs (no need to build an infrastructure). Some of theapplications in MANETs are Military Tactical Operations, Search and Rescue Operations,Disaster Relief Operations.MANEThas thefollowing challenges like Limited bandwidth, Dynamic topology, Routing OverheadPacket losses due to transmission errors.Solution to overcome wormhole attack in an attacker records packets at one location of the network, tunnel them to another location and retransmits them there into the network.The wormhole attack allows attackers togain unauthorized access,Disrupt routing,Perform DOS attack.A new routing protocol naming **E**xtended **P**rime**P**roduct **N**umber (**EPPN**) based on the hop count model is proposed in this article. Here hop count between source & destination is obtained depending upon the current active route.This hop count model is integrated into AODV protocol. In theproposed scheme firstly the route is selected on the basis of RREP and then hop count model calculates the hop count between source & destination. Finally wormhole DETECTION procedure will be started if the calculated hop count is greater than the received hop count in the route to get out the suspected nodes.

Index Terms :Dynamic topology, Routing Overhead Packet, Disrupt routine.

1.INTRODUCTION

The first generation of ad hoc network goes back to 1972. At that time, they were called PRNET (Packet Radio Networks). The history of ad-hoc networks can be dated back to the DoD1-sponsored Packet Radio Network (PRNET) research for military purpose in 1970s, which evolved into the Survivable Adaptive Radio Networks (SURAN) program in the early 1980s [1]. In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad-hoc networks emerged in 1980s, when the ad-hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks.

In the 1990s, the concept of commercial ad-hoc networks arrived with note-book computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences. Since mid-1990s, a lot of work has been done on the ad hoc standards. Within the IETF, the MANET working group was born, and made effort to standardize routing protocols for ad hoc networks. Meanwhile, the IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated.

Some of the challenges in MANET are listed as follows:
1) Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
2) Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.
3) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
4) Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.
5) Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.
6) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.
7) Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.
8) Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

In this paper, hop count based routing scheme has been presented to mitigate the wormhole attacks in ad hoc networks. During Wormhole attack, an attacker uses a pair of nodes connected in a manner. It can be named as a special private connection over the MANETs [2]. The main aim is to make a short circuit in the network to create some routing problems.

2. REVIEW OF LITERATURE

In the paper "A secure Routing Protocol for ad hoc Networks B.Dahil,B.Levine,E.Royer and C.Shields[1]",The security threats against ad hoc routing protocols is discussed by examining AODV and DSR.ARAN protocol is able to successfully identify on attack. In the existing paper causes of attacks and methods of depicting it are successfully carried out by ARAN. In our paper, variousreasons for wormhole attack is known through this paper the methods to attack it is also known which incorporated in our paper.

As given in the paper "Packet Leashes: A defense Against wormhole attack in wireless ad hoc networks Y.Hu.A.Perrig,and.Johnson[2]",wormhole attack is severe attack in MANET which cannot be compromised so easily packet leashes is a mechanism by which wormhole attack is defended effectively.The defending mechanism of packet leashes is explored and incepted in our paper.

The concept of offline configuration and heavy computation in the scares resources and dynamic environment is not suitable. So on effective trust based solution are possible which is mentioned in "Trust Based Routing Mechanism in MANET: Design and Implementation Tameem Eissa, Shukor Abdul Razak, Rashid Hafeez Khokhar and Normalia Samian [4]".

The evolutionary algorithm which is dynamic by nature is adapted in AHP(Analytical Hierarchy Process)which handles the routing scheme of wireless multi hop network effectively this is mentioned in this paper"Dong-YouChoi andSeungjo Han.Robust and Secure Routing scheme for wireless multi hop network Binod Vaidya ,Sang-Soo Yeo[6]"

3.PROPOSED SYSTEM

The EPPN scheme is AODV based reactive routing scheme and it can protect against wormhole attacks during communication process and packet forwarding. In the communication process setup of EPPN scheme, an intermediate node will ensure a secure route that restrict the participation of a node with wrong replied information and whose PPN is not fully divisible [12]. Due to the scheduled continuous monitoring of nodes, the malicious nodes will be avoided by other well behaving nodes in the network. The proposed EPPN scheme binds some meta-information with RREQ & RREP packets in comparison to AODV, which results in modified message format.

A.RREQ Packet

RREQ in EPPN scheme is same as the AODV shown in Fig. 1.

Types	J	R	D	G	U	Reserved	Hop count
RREQ ID							
Originator IP Address							
Originator Seq Number							
Destination IP Address							
Destination Seq Number							

Figure 1:RREQ packet in EPPN

B. RREP Packet

In the proposed scheme RREP has additional Node IDs, Prime Product Number and computed MAC code fields shown in Fig. 2.

Types	R	A	Reserved	Prefix Size	Hop count
Source IP Address					
Destination IP Address					
Destination Seq Number					
Life tune					
Node IDs		Prime Product Number		Computed Mac Code	

Figure 2. RREP packet in EPPN

Node IDs field is used to store IDs of all the nodes from destination to source in the path, Prime product number is used to store the prime product of all the nodes from destination to source in the path. In the proposed scheme, during the secure route discovery

phase the source node (SN) broadcasts a RREQ message into the network. In turn, the RREP message generated by intermediate node (IN) includes its identity (ID), product of all prime numbers from destination to source node in the form of Prime Product Number (PPN), Hop count and computed MAC code using a secret shared key between itself and the destination node.

Upon receiving the RREP message from IN, SN decrypt the MAC [11] and examines the PPN i.e. it divides the PPN with the IDs of nodes mentioned in RREP and calculates the hop count named as he. As RREP packet contains the hop count value (hr), that value is retrieved by SN. SN compares hr and he. If he> h_c the SN will mark the path with the prediction of wormhole. The SN temporarily enables the route in which node is marked as wormhole

C. Hop Count calculation

252 In EPPN, the SN is required to calculate the hop count from source to destination based on the PPN. Simple division operation for our hop count calculation is adopted. Based on the model, given the PPN and IDs of all the nodes between the source and destination in the path, the SN can calculate the hop count to the destination. Algorithm for hop calculation is shown in algorithm 1.

D. Wormhole DETECTION

Once the SN predicts that the wormholes lies somewhere in the received route its next goal is to find the two ends of the wormhole. In the process of further identification of the two ends of the wormhole, the SN initiates wormhole DETECTION process. The SN forwards a DETECTION packet along already marked path by itself. To avoid the wormhole in future communication all the nodes will be updated at the end of DETECTION phase.

Algorithm 1 Hop count calculation between source and destination

input: PPN, id of nodes
output: h_c
1. $h_c = 0$, n=1
2. while (PPN!= I)
3. PPN=PPN/idn
4. he++
5. n++
6. end

The INs in turn, responds with DETECTION-RESPONSE packet to the SN including the following 3 fields:

(i) IDs of all the nodes in backward route from IN to SN
(ii) PPNumber i.e. the product of prime numbers from destination node to the source node.
(iii) Computed MAC code using a secret shared key between itself and the destination

Each IN forwards the DETECTION packet to the next hop. Finally the DN drops the DETECTION packet when it reaches to the DN and acknowledges the SN. With the help of algorithm 1 the SN calculates the hop count between the SN and each IN. In this way the SN crosschecks the hop count difference at each IN along the route from the SN to DN. An increase in hop count ensures that a wormhole is present in the route.

Further the SN has to identify the exact location of the wormhole. In this process the SN determines that a wormhole is present where the difference occurs. The whole scenario of wormhole identification in AODV routing protocol is depicted in figure 3.

Algorithm 2 Route selection with worm hole detection

1. SN broadcast RREQ packet to every neighbor node and receive RREP with in time T, RREP will be select among various reply having largest sequence number & minimum hop count and all other RREP buffered at source node.
2. SN decrypts the selected RREP, retrieves the hop count value from the received RREP packet and calls hop count calculation procedure.

If $h_r >= h_c$

SN starts data transmission.

else

SN predicts a wormhole attack and wormhole DETECTION procedure will be launched. To the nodes with identified wormhole SN broadcast an ATTACK message into the network, to communicate further SN also select a shortest route from the buffered RREP.

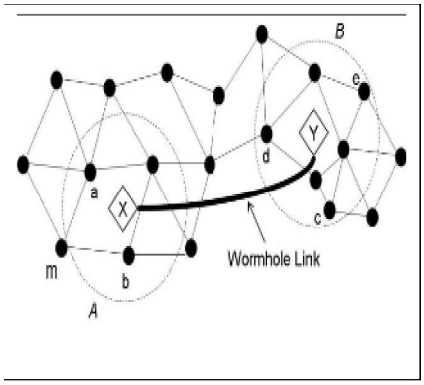
Consider a MANET in Fig. 3 with 11 nodes, where nodes WI & W2 are the wormholes. The graph denotes a shortest path from SN to DN. Each SN maintains an association table. The association table has three rows as shown in table 1. First row denotes the received path 11 - 47- 67- 29- 71- 31- 17- 79- 13; next row indicates the corresponding hop count to each intermediate and the destination node. Then calculated hop counts are shown in the last row. SN refers to algorithm 1 to calculate the hop count between the SN and each IN. From table 1, it can be seen that a peak increase (the hop count increases from 3 to 7) at node 29.

Algorithm 3 Wormhole DETECTION

1. SN forwards a DETECTION packet along the path that has been marked by it.
2. Upon receiving a DETECTION packet, intennediate nodes (IN) replies a DETECTION-RESPONSE packet to the SN with its ID, PPN & computed MAC code using a secret shared key between itself and DN.
3. After getting DETECTION packet, the DN drops the packet and send acknowledgement to the SN.
4. The SN calls hop count calculation procedure to determine the smallest hop count (he) between the SN & IN.
5. A peak increase in hop count observed by SN ensures that a wormhole presents between the nodes.

The source node will verify the nodes integrity and affirms that the wormhole lies somewhere in between node 29 and node 79. WI & W2 are marked as wormhole and due to the presence of wormhole, node 29 &79 become neighbors. After locating the wormhole, the source initializes an ERROR message to broadcast the two areas into the network

WORMHOLE DETECTION



4.CONCLUSION

Thus In this work, a novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits of our research work, we plan to investigate the following issues in our future research: 1) possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature; 2) examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre distributed keys; 3) testing the performance of EAACK in real network environment instead of software simulation.

REFERENCE

[1] B. Dahill, B. Levine, E. Royer and C. Shields, "A secure routing protocol for ad hoc networks," in Proc. [CNP '02, 2002, p. 78-89.

[2] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc network," in Proc. CNDS '02, 2002, p. 1-13.

[3] Radha Poovendran and Loukas Lazos, " A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," ACM Journal on Wireless Networks (WINEJ], vol. 13, pp. 27 - 59, Oct. 2007.

[4] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, " L1TEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," in ProG. DSN'05, 2005, p. 612-621.

[5] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad hoc Networks," in ProG. ACCT '12, 2012, p. 556-560.

[6] J. Eriksson, S. Krishnamurthy, and M. Faloutsos," Truelink: A practical countermeasure to the wonnhole attack," in ProG. ICNP'06, 2006, p. 75- 84.

[7] N. Bhalaji and A. Shanmugam, "Dynamic Trust based method to mitigate grehole attack in Mobile adhoc networks," in ProG. ICCTSD '} 1,2011, p. 907-914.