Detection of Wormhole Attack in Mobile Ad-hoc Network using Hash Compression Function

[1]Rachna Vitthalapara, [2]Mayank Guar
[1,2]Dept.of Computer Engineering, SOCET, GTU, Gujarat, India

Abstract
Mobile Ad-hoc Network (MANET) has become an undividable and acceptable part for communication for mobile equipments. One of powerful form of attacks is Wormhole attack that affects on the network layer. In this work, the techniques dealing with wormhole attack are surveyed and a methodology for wormhole detection is proposed. Inwormhole attack, a malicious node records data packets at one location in the network and tunnels them to another malicious node far away, which retransmits them into the network locally. Our approach is based on the Hash based Compression Function (HCF) which will use any secure hash function to compute a value of hash field for RREQ packet in AODV. Proposed methodology looks very promising compared to other solutions proposed in literature. The proposed methodology will be incorporated in AODV routing protocol and will be implemented and simulated in NS2.

Keywords
MANET, AODV, Security, Throughput, Wormhole Attack, Detect Attack

I. Introduction

Ad-hoc in Latin means for this purpose only, Mobile Ad hoc Network (MANET) is a collection of mobile nodes communicating with each other without any centralized system. Mobile Ad network is a self-configuring infrastructure less network of mobile device connected without any wires. Mobile Ad hoc network in which each mobile device that can be set up dynamically anywhere and any direction. In MANET each node acts as a not only host but also acts as a router same time to forward packets. In MANET each mobile device free to Move in any direction independently. MANET is used when any backbone infrastructure is absent, destroy, impractical or not visible [1]. Routing in MANET is difficult due to node mobility, lack of predefined infrastructure, limited transmission rang. Presence of malicious node can disrupt the functioning of routing Protocol. Security is must to make the network and routing protocol work properly. There are various attack on wireless channels like blackhole attack, wormhole attack etc.

II. Wormhole Attack

This attack is done with two or more nodes.Nodesapper apart but they are within a single hop distance. Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunnelling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighbouring information [2].

A. Types of Wormhole Attack [3]

Number of nodes involved in establishing wormhole and the way to establish it classifies Wormhole into the following types.

1. Wormhole using Out-of-Band Channel

In this two-ended wormhole, a dedicated out-of-band high bandwidth channel is placed between end points to create a wormhole link.

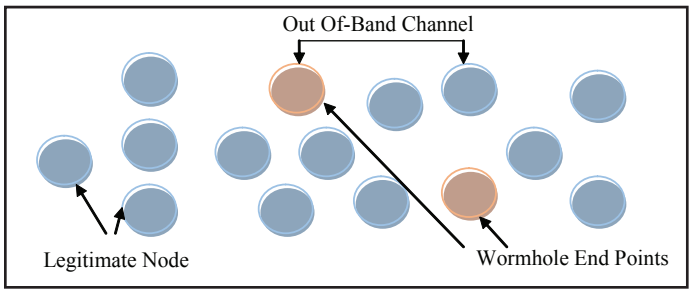

Fig. 1: Wormhole Using out-of-band Channel and Encapsulation [3]

2. Wormhole using Packet Encapsulation

Each packet is routed via the legitimate path only, when received by the wormhole end, gets Encapsulated to prevent nodes on way from incrementing hop counts. The packet is brought into original form by the second end point.

3. Wormhole using High Power Transmission

This kind of wormhole approach has only one malicious node with much high transmission Capability that attracts the packets to follow path passing from it.

4. Wormhole using Packet Relay

Like the previous approach, only one malicious node is required that replays packets between two far nodes and this way fake neighbour are created.

III. Proposed Work

This paper Proposed a novel technique to detect wormhole attack. which is based on the AODV Protocol can detect wormhole attack in the network in an efficient manner.

Our methodology is based on the Hash based Compression Function (HCF) which is actually using any secure hash to compute a value of hash field for RREQ packet. Source node S initialize Hash based Compression Function (HCF) e.g. SHA-1 and Source node S also initializes Seed Field &value of Hash Field, appends it with RREQ and forwards it to itsneighbor. If neighbor equal to destination then destination node D applies HCF, No. of hop count times on seed value. Otherwise each valid intermediate node will apply HCF on hash field and appends it with RREQ and forward it to its neighbors.

Destination node D receives multiple route requests. If computed hashed value equal to appended hashed value then destination D replies RREP (route reply) on Destination D applies HCF, No. of hop count times on Seed value. If Computed Hashed Value not equal to Appended Hashed Value then Destination D detects that RREQ comes from tunnel and neighbor m2 detected as a wormhole attacker. Destination D sets flag = 1 (extra field) in RREP and replies it via tunnel path. Source node S receives RREP

with flag =1 and detects neighbor m1 as a wormhole attacker.

B. Proposed Algorithm

1. Detection of Wormhole Attack in Mobile Adhoc Network

1. Source node S starts route discovery to locate Destination node D.
2. Source node S initialize Hash based Compression Function (HCF) e.g. SHA-1
3. Source node S also initializes Seed Field & value of Hash Field, appends it with RREQ and forwards it to its neighbors.
4. If (Neighbor == Destination)
   {
   Goto step 5.
   }
   Else
   {
   Each valid intermediate node will apply HCF on Hash Field & appends it with RREQ and forwards it to its neighbors.
   Goto step 4.
   }
5. Destination node D receives multiple route requests (RREQs).
6. Destination D applies HCF, No. of hop count times on Seed value.
7. If (Computed Hashed Value == Appended Hashed Value)
   {
   Destination D replies RREP (route reply) on path having minimum hop count
   }
   Else
   {
   1. Destination D detects that RREQ comes from tunnel and neighbor m2 detected as a wormhole attacker
   2. Destination D sets flag = 1 (extra field) in RREP and replies it via tunnel path
   3. Source node S receives RREP with flag =1 and detects neighbor m1 as a wormhole attacker
   }

IV. Simulation and Comperission

We have used NS-2 for simulating various aspect.In this Paper We have taken 25 nodes. Parameters taken are listed in table given below:

Table 1: Simulation Parameters

Parameter		Value
Simulator		NS-2(Version 2.34)
Channel type		Wireless
Radio-propagation model		Propagation / TwoRayGround
Network interface type		Phy/WirelessPhyExt, Phy/WirelessPhyExt
MAC Type		Mac /802.11
Interface queue Type		CMUPriQueue
Link layer type		LL
Antenna model		Antenna/Omni Antenna
X dimension of the topography		1000
Y dimension of the topography		1000
Max packet in ifq		50
Number of mobile nodes		25 Nodes
Traffic Type		UDP, CBR
Routing Protocols		AODV

Table 1 shows the simulation parameters like channel type, Radio-propagation model, MAC type etc. and their values for the simulation of Normal AODV, Wormhole AODV and Proposed AODV.

V. Results

A. Packet Information

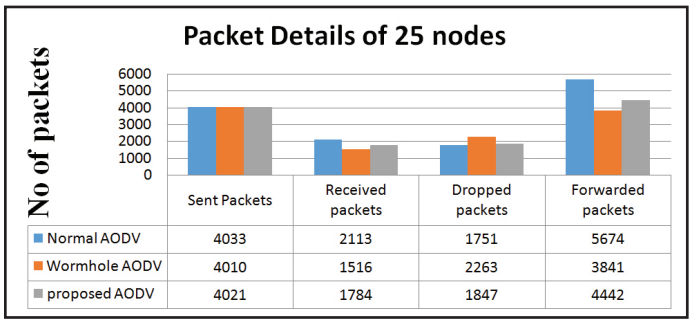

Fig. 2: Packet Information of 25 Nodes

Fig. 2 shows that wormhole AODV has more packets dropping than the Normal AODV. But by using the Proposed AODV, we can reduce the packet dropping than the wormhole AODV.

1. Delivery Rate

It is the number of packet received by destination node divided by number of packets send by source node .Delivery rate is lower in case of wormhole attack.so presence method increase delivery rate shown in fig.

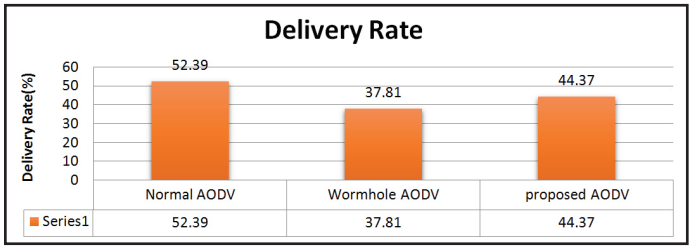

Fig. 3: Delivery Rate

B. Average End to End Delay

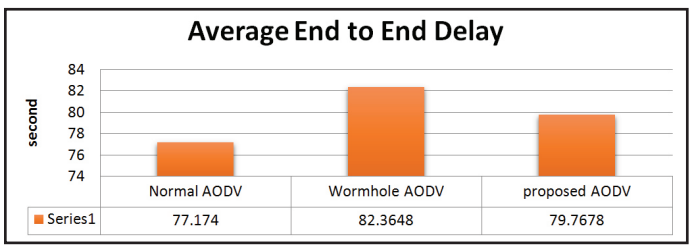

Fig. 4: Average End to End Delay of 25 Nodes

Fig. 4 shows, Average End to End Delay of wormhole AODV is increase than the Normal AODV. But by using the Proposed AODV, we can decrease the Average End to End Delay than the Wormhole AODV.

C. Throughput

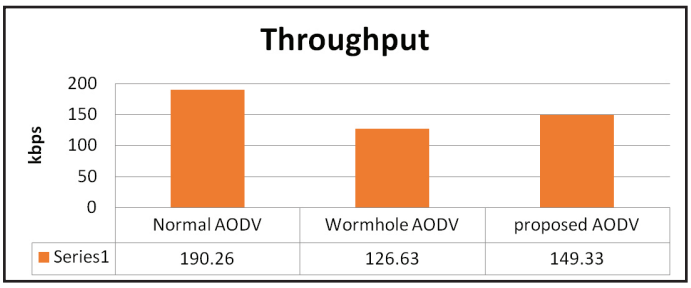

Fig. 5: Throughput of 25 nodes

Fig. 5 Shows, throughput of wormhole AODV is reduced than the Normal AODV. But by using the Proposed AODV, we can increase throughput than the Wormhole AODV.

VI. Conclusion

When the wormhole attack is initiated, the attackers can capture data packets on either side, forward them through the wormhole link and rebroadcast them on the other node and finally tries to disturb the normal routing procedure.In this work, I have proposed a wormhole detection mechanism to detect against wormhole attacks. In proposed method wormhole nodes are detected. Also the information of detected nodes is broadcasted to all other nodes to delete the entries of detected wormhole nodes from their routing table. The proposed mechanism is incorporated in AODV routing protocol and implemented and simulated in NS2. After the analyses of simulation results it is found that proposed wormhole detection mechanism detects wormhole attack.

Reference

[1] Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong,"Security in Wireless Sensor Networks: Issues and Challenges", ICACT2006, pp. 1043-1048
[2] [Online] Available: http://www.ijettjournal.org
[3] Dhara Buch, Devesh Jinwala,"Prevention of wormhole attack in wireless sensor network", IJNSA 2011, pp. 85-98.
[4] Ravinder Ahuja, Alisha Banga Ahuja, Pawan Ahuja, "Performance Evolution and Comparison of AODV and DSR Routing Protocols in MANETs under Wormhole Attack", IEEE 2013, pp. 669-701.
[5] Umesh Kumar Chaurasia, Mrs.Varsha Singh,"Modified wormhole detection AODV protocol.[IEEE 2013],pages 239-243
[6] Saurabh Gupta, SubratKar, S Dharmaraja,"[WHOP] Wormhole attack detection protocol using hound packet", IEEE 2011, pp. 226-231.
[7] [Online] Available: http://www.cs.jhu.edu/~cs647/intro_adhoc.pdf
[8] Mukesh Kumar, Rahul Rishi, D.K.Madan,"Issue and challenges of quality of service in mobile adhoc network", IJCSET, pp. 61-66.
[9] Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong,"Security in Wireless Sensor Networks: Issues and Challenges", ICACT2006 pp. 1043-1048