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. 3, Issue 11, November 2015

Improvement in Reduce the Load of Processing Risk from Security Using AODV Routing Protocol

S. Sathish Raja, S. Saravana Kumar

Research Scholar, Dept. of CSE, Vels University, Chennai, India

Professor, Dept. of CSE, SVEC, India

ABSTRACT : In this research paper an ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. As routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. Our objective is to find out the malicious node that performs the wormhole attack in network. We have assumed that the MANET consists of group of nodes. We have proposed an algorithm where intrusion detection has been done in a group based manner to take care of the wormhole attacks. The AODV routing protocol is used as the underlying network topology. A two layer approach is used for detecting whether a node is participating in a wormhole attack. The layered approach is introduced to reduce the load of processing on each group heads. From security point of view, this will also reduce the risk of a group head being compromised.

KEYWORDS: AODV, Security, MANET, Protocol, Attack, Intrusion , Detection

I.INTRODUCTION

WORM HOLE ATTACK

In this section we explain the wormhole attacks modes and classes while pointing to the impact of the wormhole attack and the efforts that have been done in the literature to detect and prevent this attack.These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan [15] on individual layer are as under.
Application Layer: Malicious code, Repudiation,
Transport Layer: Session hijacking, Flooding
Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.

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. 3, Issue 11, November 2015

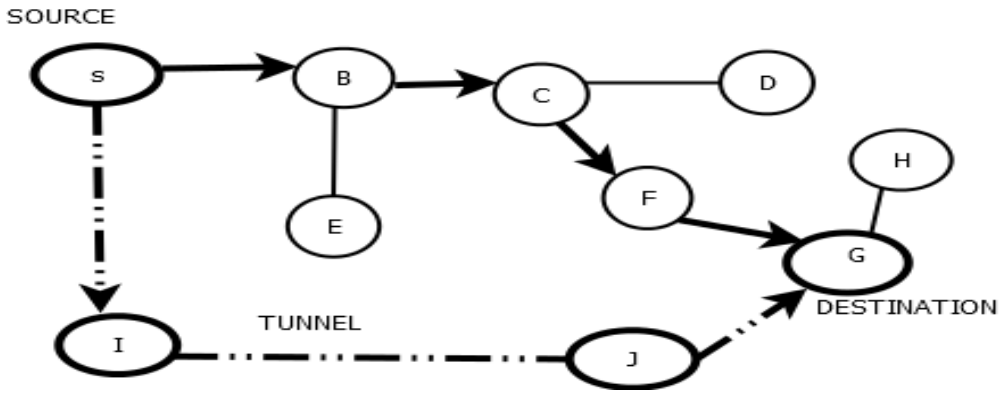

Figure 1- Node transmission from source to destination

II.PROPOSED METHODOLOGY

Our objective is to find out the malicious node that performs the wormhole attack in network. We have assumed that the MANET consists of group of nodes. The assumptions regarding the organization of the MANET are listed following section.

2.1 PROPOSED ARCHITECTURE

The following assumptions are taken in order to design the proposed algorithm.

1) A node interacts with its 1-hop neighbors directly and with other nodes via intermediate nodes using multi-hop packet forwarding.
2) Every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.
3) The entire network is geographically divided into a few disjoint or overlapping groups.
4) The network is considered to be layered.
5) Each group is monitored by only one group head (monitoring node).

2.2 GROUP FORMATION

We have proposed an algorithm where intrusion detection has been done in a group based manner to take care of the wormhole attacks. The AODV routing protocol is used as the underlying network topology. A two layer approach is used for detecting whether a node is participating in a wormhole attack. The layered approach is introduced to reduce the load of processing on each group heads. From security point of view, this will also reduce the risk of a group head being compromised.

The entire network is divided in group . The group may be overlapped or disjoint. Each group has its own grouphead and a number of nodes designated as member nodes. Member nodes pass on the information only to the group head. The group-head is responsible for passing on the aggregate information to all its members. The group head is elected dynamically and maintains the routing information.

WN is the ward node, used for monitoring the malicious activity. The main purpose of the ward node is to save the group from possible attacks. The ward node has the power to monitor the activity of any node within the group. The ward node reports to the group head of the respective layer in case a malicious activity is detected. A group head detects a malicious activity and informs the group head of the outer layer to take appropriate action. It's the duty to check the number of false routes generated by any node. The group head of outer layer takes upon itself the responsibility of informing all nodes of the inner layer about the malicious node.

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. 3, Issue 11, November 2015

III.DETECTION TECHNIQUE OF WORMHOLES

Before, we present the actual algorithm for detection of wormhole attacks, the data structure used for the purpose has been described below.

1**. Threshold tolerance (P_{th}):** This refers to the threshold value defined by the monitoring node. It is the tolerance value for lost packets.
2**. Expected route trip time (T_e)**:Expected route trip time of a packet to a destination node is calculated as the time taken when the source node send HELLO packet to the destination node and get back an acknowledgement for that.
3**. Route trip time (T_r):** When the source node send packet it starts a timer. On receipt of an acknowledgement, the timer is stopped. The total time elapsed is recorded as Tr
4**. P_s**: Number of packets sent to a destination node D from source node S.
5**. P_d**: Number of packets received by node D from a specific source node S.

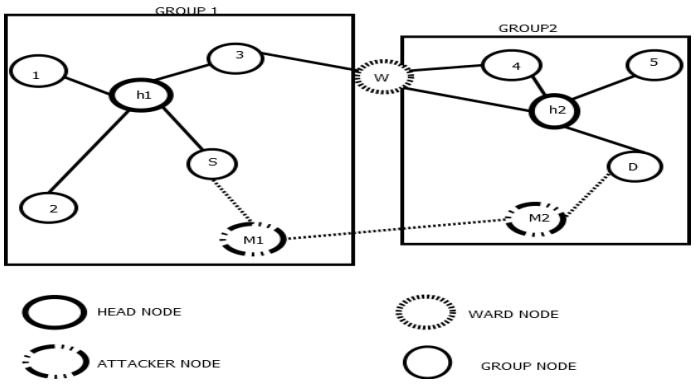

Figure 2- Group Based Detection Technique

In figure node S sends a HELLO message for destination node D. S has a path to D via (2, 3). M1, being in the proximity of S, overhears the HELLO message and forwards the same to node M2 in the other end of the network. Node D hears this HELLO message from S and therefore considers S to be its immediate neighbor and follow the route to send message to S via M1 and M2. The node 3 which is at the overlapping position of two group acts as WARD node who can here every packet send by node S for the destination node D and monitor the packets route from souce to destination. The ward node is also called monitoring node. When S observes some malicious behavior when it sends packet to D it informs the ward node. The ward node then checks the number of packets send for the node D and those actually received by D from S. Then it calculates $\Delta p = P_s - P_r$. If the value of Δp exceeds the threshold value P_{th} that is predefined by the monitoring node then monitoring node finds out the wormhole attack.

3.1 PROCEDURE OF WORMHOLE DETECTION

Begin
Step-1 Initiate the network with two groups and each group have some nodes.
Step-2 The node within a group having minimum node id becomes group Head. The node id for each node is provided when the node enter into the group.
Step-3 The node nearest to both the group head is chosen as the ward node.
Step-4 Source S sends hello message to the intermediate node with destination node ID .

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. 3, Issue 11, November 2015

Step-4.1 Source S initialise timer at T_1.
Step-4.2 When destination receives packet it unicast the acknowledgement to the Source S.
Step-4.3 When acknowledgement receives by source S then it records time T_2.
Step-4.4 Now we calculate expected route trip time T_e as [$T_e = T_2 - T_1$]
Step-4.5 Source S sends packet to destination node and it records t_1 at the time of sending the packet (at source) and then records t_2 at the time when source receives acknowledgement from the destination node.
Step-4.6 Now calculate route trip time as [$T_r = t_2 - t_1$]
Step-4.7 Now we compare route trip time T_r with expected route trip time T_e And check for $T_r << T_e$
Step-5 Then the ward node checks packets sent by source (P_s) and packets received by destination(P_r).
Step-6 calculate [$\Delta p = P_s - P_r$]
Step-7 We compare Δp which could be Drop with the threshold value $P_{th.}$
Step-8 If ($\Delta p > P_{th}$) then inform the source node to stop packet transfer
Step-9 the source node stop packet transfer inform group head.
End

3.2 Link Time Delay Management

One goal of our protocol is fault avoidance. This is achieved by the route discovery phase based on weights associated with each link. The link weight management component of the protocol maintains a weight list for links discovered by the fault detection algorithm and uses a multiplicative increase scheme to penalize links. . We refer to the set of nodes required to send acknowledgments as probed nodes, or for short probes. The list of probes is specified on legitimate traffic. Thus, an adversary is unable to drop traffic without also dropping the list of probes and eventually being detected

IV. CONCLUSION

a new group based wormhole detection method has been proposed. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack. A number of recent works have been studied before proposing this new methodology. The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers. or extremely accurate clocks, etc. Currently more studies are being done to analyze the performance of the proposed algorithm in presence of multiple attacker node.

REFERENCES

[1] : Wormhole Attacks in Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006
[2] : IN THE PAPER Detection and Prevention of Layer-3 Wormhole Attacks on Boundary State Routing in Ad hoc Networks. 2010 International Conference on Advances in Computer Engineering
[3] Y.C. Hu A. Perrig and D. B. Johnson. PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks.
IEEE INFOCOM, pages 1976–1986, 2003. 612–621, 2005
[4] : H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, pages 6–11, January 2006..
[5] : Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks. Computer Security, vol.29, March 2010.
[6] : S Dharmaraja and Subrat kar:WHOP: Wormhole Attack Detection Protocol using Hound Packet . 2011 international conferenceon innovation in information technology
[7]. On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, Conference on Security and Privacy for Emerging Areas Communications, SecureComm 2005, September2005.
[8]. I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweightcounter measure for the wormhole attack in multihop wireless networks. International Conference on Dependable Systems and Networks, pages 612–621, 2005.
[9]: Issa Khalil, Saurabh Bagchi & Ness B. Shroff, "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks".http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4198824

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. 3, Issue 11, November 2015

[10] *:* A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks
2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.1

[11] C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002.
[12]: P. Gupta and P.R. Kumar. Capacity of wireless networks. IEEE Transactions on Information Theory, Volume 46, Issue 2, March 2000, doi:10.1109/18.82579.
[13]: Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris, Capacity of Ad Hoc Wireless Networks, in the proceedings of the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001.
[14]: Wu S.L., Tseng Y.C., "Wireless Ad Hoc Networking, Auerbach Publications", 2007 ISBN 978-0-8493-9254-2.
[15]: Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.
[16] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks," Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2,pp. 370- 380, 2006.
[17] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", in *proceedings of INFOCOM*, 2004.
[18] W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, "Defending agains Wormhole Attacks in Mobile Ad Hoc Networks," Wireless Communication and Mobile Computing, January 2006.
[19] M.A. Azer S.M. El-Kassas A. Wahab F Magdy S and El-Soundani. Intrusion detection for wormhole attacks in ad hoc networks a survey and a proposed decentralized scheme.
In the proceedings of the IEEE international conference on availability, reliability and security, pages 630–646, 2008.
[20] G. Lee D. Kim and J. Seo. An approach to mitigate wormhole attack in wireless ad hoc networks. *In the proceedings of the international conference on information security and assurance*, pages 220–225, 2008.
[21] Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks. *Computer Security*, vol. 29, March 2010.
[22] Y.C. Hu A. Perrig and D. B. Johnson. *PACKET LEASHES*: A defense against wormhole attacks in wireless ad hoc networks. *IEEE INFOCOM*, pages 1976–1986, 2003.