Journal of Engineering and Applied Sciences 13 (5): 1235-1238, 2018
ISSN: 1816-949X

Efficiently Process in Reducing the Load Risk from Security Using ABR (Associate-Based Routing) Routing Protocol

[1]S. Sathish Raja and [2]S. Saravana Kumar
[1]Department of CSE, Vels University, Chennai, India
[2]Department of CSE, Karpagam College of Engineering, Coimbatore, India

Abstract: 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 classicrouting, ad-hoc networks can usefloodingfor forwarding the data. The 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 ABR 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. In this study, presents a new, simple and bandwidth-efficient distributed routing protocol to support mobile computing in a conference size ad-hoc mobile network environment. Unlike the conventional approaches such as link-state, distance-vector distributed routing algorithms and TORA, the protocol does not attempt to consistently maintain routing information in every node. We employ an associativity-based routing scheme where a route is selected based on nodes having associativity states that imply periods of stability. In this manner, the routes selected are likely to be long-lived and hence there is no need to restart frequently, resulting in higher attainable throughput. To discover shorter routes and to shorten the route recovery time when the association property is violated, quick-abort mechanisms are incorporated into the protocol. The protocol is free from loops, deadlock and packet duplicates.

Key words: ABR, security, MANET, protocol, attack, intrusion detection

INTRODUCTION

Wormhole attack: In this study, we explain the worm hole 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 his 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 Krag and Buettrich (2004), on individual layer are as under:

- Application layer: malicious code, repudiation
- Transport layer: session hijacking, flooding
- Network layer: sybil, flooding, black hole, grey hole wormhole, link spoofing, link withholding, location disclosure, etc. (Fig. 1).

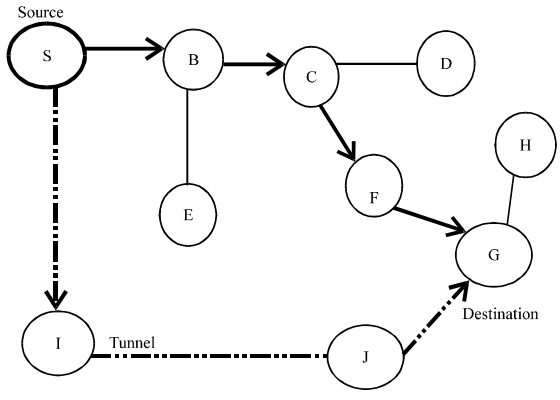

Fig. 1: Node transmission from source to destination

MATERIALS AND METHODS

The objective is to find out the malicious node that performs the wormhole attack in network. We have

Corresponding Author: S. Sathish Raja, Department of CSE, Vels University, Chennai, India

assumed that the MANET consists of group of nodes. The assumptions regarding the organization of the MANET are listed following section.

Proposed architecture: The following assumptions are taken in order to design the proposed algorithm:

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

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 (Jain and Kandwal, 2009). The ABR 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 (Hu *et al*., 2003). 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 group head and a number of nodes designated as member nodes (Su, 2010). 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 (Chiu and Lui, 2006).

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 (Azer *et al*., 2008). 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.

RESULTS AND DISCUSSION

Detection technique of wormholes: Before, we present the actual algorithm for detection of wormhole attacks (Poornima *et al*., 2010) the data structure used for the purpose has been described below.

Threshold tolerance (P_{th}): This refers to the threshold value defined by the monitoring node. It is the tolerance value for lost packets.

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.

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.

P_s: Number of Packets sent to a Destination node D from Source node S.

P_d: Number of Packets received by node D from a specific Source node S. Figure 2 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 (Toh, 2002). The ward node is also called monitoring node. When S observes some malicious behavior when it sends packet

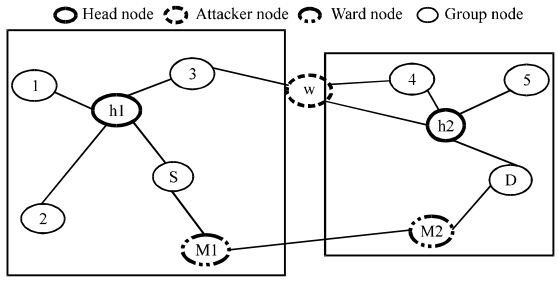

Fig. 2: Group based detection technique

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.

Algorithm; 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

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

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 (Khalil *et al*., 2005). 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 (Awerbuch *et al*., 2005). We refer to the set of nodes required to send acknowledgments as probed nodes or for short probes (Azer *et al*., 2008). 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.

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

Awerbuch, B., R. Curtmola, D. Holmer, H. Rubens and C.N. Rotaru, 2005. On the survivability of routing protocols in ad hoc wireless networks. Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, September 5-9, 2005, IEEE, Athens, Greece, ISBN:0-7695-2369-2, pp: 327-338.

Azer, M., S.E. Kassas, A.W. Hassan and M.E. Soudani, 2008. Intrusion detection for wormhole attacks in ad hoc networks: A survey and a proposed decentralized scheme. Proceedings of the 3rd International Conference on Availability, Reliability and Security, March 4-7, 2008, IEEE, Barcelona, Spain, ISBN:978-0-7695-3102-1, pp: 636-641.

Chiu, H.S. and K.S. Lui, 2006. DelPHI: Wormhole detection mechanism for ad hoc wireless networks. Proceedings of the 1st International Symposium on Wireless Pervasive Computing, January 16-18, 2006, IEEE, China, ISBN:0-7803-9410-0, pp: 1-6.

Jain, M. and H. Kandwal, 2009. As survey on complex wormhole attack in wireless ad hoc networks. Proceedings of the International Conference on Advances in Computing, Control and Telecommunication Technologies, December 28-29, 2009, IEEE, Trivandrum, Kerala, India, ISBN:978-1-4244-5321-4, pp: 28-29.

Khalil, I., S. Bagchi and N.B. Shroff, 2005. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. Proceedings of the International Conference on Dependable Systems and Networks, June 28- July 1, 2005, IEEE, Yokohama, Japan, ISBN: 0-7695-2282-3, pp: 612-621.

Krag, T. and S. Buettrich, 2004. Wireless Mesh Networking. O'Reilly Media, Boston, Massachusetts.

Poornima, E., C.S. Bindu and S.K. Munwar, 2010. Detection and prevention of layer-3 wormhole attacks on boundary state routing in ad hoc networks. Proceedings of the International Conference on Advances in Computer Engineering (ACE), June 20-21, 2010, IEEE, Bangalore, India, ISBN:978-1-4244-7154-6, pp: 48-53.

Su, M.Y., 2010. WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Comput. Secur., 29: 208-224.

Toh, C.K., 2002. Ad Hoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall, Upper Saddle River, New Jersey, USA.