International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Wormhole Attack Detection By using Trustbased Routing In Wireless Networks

V. Vasantharasi

Computer Science and Engineering, IFET College of Engineerimg, Villupuram, TamilNadu, India

ABSTRACT

Network security has been shown to be an effective approach to improve the wireless system performance. However many security issues impede its wide deployment. DAWN against wormhole in wireless network systems. The network has to avoid the attacker nodes. This can be achieved by trust based mechanism. Level Based upon the assigned trust value.

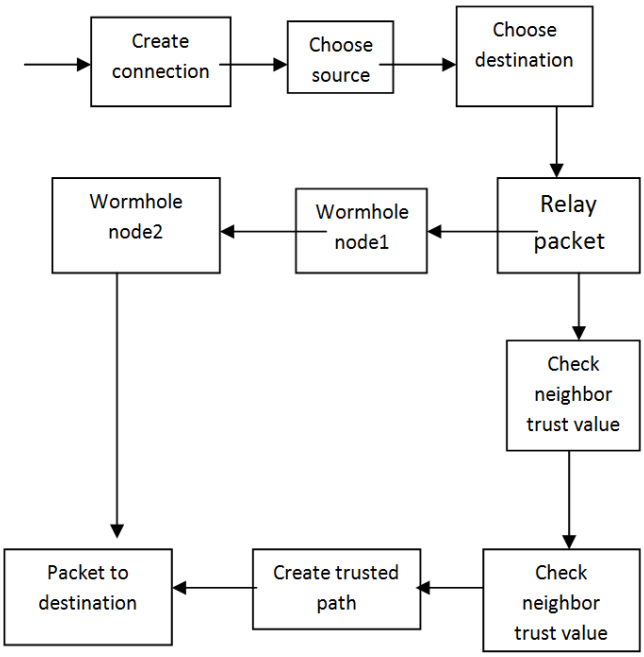
Keywords: Wireless network, DAWN algorithm

I. INTRODUCTION

In the effort to improve the system performance of wireless networks, network coding has been an effective and promising approach and it constitutes a fundamentally different approach compared to traditional wireless networks, where intermediate nodes store those packets and forward them as the original. In contrast, in wireless network systems, the forwarders are allowed to apply encoding schemes on what they receive, and then they start to create and transmit a new packet in network. The idea of mixing packets on each node takes good advantages of the opportunity diversity and broadcast nature of wireless communications, and significantly enhances system performance and attacks, whose impact and counter measures are still not well understood because their underlying characteristics vary in a whole from completely-studied traditional wireless networks. The wormhole attack is one of these attacks. In a wormhole attack, the attacker can forward each packet using wormhole links and without modifying the packet transmission by routing it to an unauthorized remote node.

II. METHODS AND MATERIAL

A. Architecture



B. Algorithm

TRUST BASED ROUTING ALGORITHM

Input: Entire network G with nodes V and their locations L, and the source node vs

Output: ETXs for all the nodes in the network G

1: ETX (vs) ← 1:0

2: for each node vi in V, except vs do

3: ETX (vi) ← þ1

4: end for

5: repeat

6: ETX updated ← false

7: for each node vi in the network G, other than vs do

8: Let N be the set of the neighbors of vi s.t. ETX (vk) < þ1 for any vk Є N

9: If ETX (vi) > 1 Then

10: ETX (vi) 1 ← 1_vkЄN

11: ETX updated ← true

12: end if

13: end for

14: until ETX updated = false

15: return the ETXs for all the node

C. Modules Description

1. Network deployment
2. One hop neighbor detection
3. Worm hole attack detection
4. Trust based routing

1. Network Deployment

Consider a wireless network containing 'N' number of nodes installed in the 2D plane of NAM animator. Each node knows its relative location and is capable of communicating with its neighboring nodes usually use geographic routing. The whole network is completely connected through many-hop communications. We consider a wireless network with N nodes. Let N denote the set of all nodes in the network. The communication among all n nodes is based on a tree topology with the destination as the root. The tree is formed in the initial phase as follows. Data are transferred along the edges in this communication tree.

2. One -Hop Neighbor Detection

A sensor network with a graph G(k)= (V(k),e(k)), whose node set V(k) represents the sensor nodes active at time k and the edge set e(k) consists of pairs of nodes (u,v) such that nodes u and v can directly exchange messages between each other at time k. By an active node we mean a node that has not failed permanently. All graphs considered are undirected, i.e., (i, j) =(j,i). The neighbors of a node i is the set Ni of nodes connected to i, i.e., Ni. The number of neighbors of is called its degree, which is denoted by di(k). A path from i to j is a sequence of edges connecting i and j. A graph is called connected if there is a path between every pair of nodes. From source node to destination node, neighbors of a source node are taken and all possible paths are created.

3. Wormhole Attack Detection

In these type of attacks, the attackers from various locations transmit packets with the help of a out-of-band tunnel. The transmission tunnel is called a wormhole link. When the wormhole attack is initiated, these attackers have the capability to capture data packets from both sides, forward them through the wormhole link and rebroadcast them on the other node.

For the centralized algorithm, a central node is set up, which owns the authority to gather information from all the nodes in the network, and run a wormhole detection algorithm based on the rank increasing information on the central node. Each active node has the responsiblity to record the time when the rank of each received packets increases gradually and then generates a report, which includes the datas such as the time of the packet, the address of node, and the rank of each node. Each node delivers the reports to the central node via common unicast.

4. Trust Based Routing

In the proposed system, routing is done dynamically. To enhance more security in the routing phase, we can include the trust factor in routing path, The routing can be taken considering node's trust factor. For example, the trust level is denoted as T. Trust value is assigned for each and every node, the numeric value such as 0 or 1 is assigned, whereas 0 is considered to be malicious node and trust value 1 is considered to be an unique node. Based upon the assigned trust value, the routing path is constructed. The node, which has trust value 1, will be included in the route rather than the node having trust level 0.

III. CONCLUSION

The impact of wormhole attacks on wireless network systems is studied. Distributed detection algorithm is proposed, which identifies wormhole node efficiently. A Centralized Algorithm that provides a centralized node to clusterize and analyze the forwarding behaviors of each node in the network, in order to react timely when wormhole attack is initiated. It is proven the exactness of the trust based routing algorithm by deriving a lower bound of the deviation in the algorithm. Also proposed a Distributed detection Algorithm against Wormhole in wireless Network coding systems. After detection of wormhole attack, the attack is avoided by using trust based routing.

IV. REFERENCES

[1]. S. Li, R. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[2]. T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[3]. S. Biswas and R. Morris, "Opportunistic routing in multihop wireless networks," ACM SIGCOMM Comput. Commun. Rev., vol. 34, pp. 69–74, Sep. 2004.

[4]. S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the air: Practical wireless network coding," in Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun., 2006, pp. 243–254.

[5]. S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun., Aug. 2007, pp. 169–180.

[6]. D. Dong, Y. Liu, X. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," IEEE Trans. Netw., vol. 19, no. 6, pp. 1787–1796, Dec. 2011.