SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 176–184

ISSN No: 2454-9614

Detecting Wormhole Attack in Wireless Network Coding Systems by using Centralized and Distributed Algorithms

S. Malathi , M. Shivakumar*, A. Padma

[a)] *Department Of Computer Science and Engineering, V.S.B Engineering College, Karur, Tamilnadu, India.*

*Corresponding Author: S. Malathi

E-mail: malathiselva92@gmail.com

Received: 10/11/2015, Revised: 15/12/2015 and Accepted: 10/03/2016

Abstract

The wireless network coding system is an efficient method to improve the performance of a wireless network. These systems have become more popular among the wireless networks. But this system also faces serious threats in the form of Wormhole attack. The wormhole attack degrades the performance of the network coding systems. In order to overcome this problem various methods have been presented. For networks with centralized authority, a centralized algorithm is used. In this algorithm, a central node gathers the information from all the nodes in the network and evaluate whether there present a wormhole link. This algorithm ranks the series of the nodes that gains the innovative packet, and uses the machine learning method to differentiate the wormhole cases. For distributed method DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems is used. In DAWN, during proper data transmissions, each node reports the irregular appearance of innovative packets and shares this with its neighbours. Moreover, DAWN assure a good successful detection rate. This existing method is more energy saving and hence decrease the implementation and communication costs

Keywords: *WSN, DAWN, Wormhole attack, ETX, Certificate authority*

1. Introduction

A wireless sensor network is a communications infrastructure for monitoring and recording conditions at various locations. The temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions are the most commonly monitored parameters. A sensor network consists of number of detection stages called sensor nodes. Each sensor node provides transducer, microcomputer, transceiver and power source. Various applications of sensor networks include industrial automation, traffic monitoring, monitoring of weather conditions, robot control and so on. Network security consists of the policies adopted to maintain the authorized access, misuse, modification

and other network-accessible resources.

Network security envelopes a variety of computer networks that is both public and private. Networks are subject to attacks. Attacks can be of two types they are "Active" and "Passive". The simplest way of preserving a network resource is by providing a unique name and a corresponding password. Network security starts with authentication. Once authenticated, a firewall enforces access policies. For networks, security management differs for all kinds of situations. With respect to this there is a special attack called wormhole attack which creates a huge impact on the network performance. The wormhole attack is quite severe and it bypasses a large amount of network traffic. In this wormhole attack the attacker can record the data packets at one location and pass it to another location. Due to the occurrence of the wormhole in the network there will be significant collapse in transmission across a wireless network. A successful wormhole attack may be the reason for disturbances and failure of a network. Proper balance between these two is necessary to prevent much consumption of resources. They can also compromise the security goals such as confidentiality and integrity.

The rest of this paper is organized as follows. We will first discuss the review of literature in Section 2, and then the proposed architecture and its brief discussion in Section 3. We evaluate our work through various experimental results in Section 4. Finally we conclude the work in Section 5.

2. Literature review

Yih-Chun Hu, Adrian Perrig, David B. Johnson says that **[1]** the promise of mobile ad hoc networks has to solve the real-world problems. It continues to grabs the attention from industrial and academic research projects. Today applications are emerging and are becoming widespread. Most previous ad hoc network research has concentrated on problems such as routing and communication, assuming a trusted environment. However, many applications run in a un-trusted environments and require secure communication and routing. Applications which require secure communications are emergency response operations, military networks, and safety-critical business operations. The mobile ad hoc network applications becomes demand, security emerges as a central requirements. Here we introduce the wormhole attack, a severe attack that is very difficult to overcome. Without compromising any nodes, the wormhole attack can be made successful. In this we introduce a new general mechanism called packet leashes. The leashes can be of geographic leashes and temporal leashes. This leash can be implemented by using a TIK (TESLA with Instant Key disclosure) protocol. The TIK protocol guarantees a security against the wormhole attack. In this the temporal leash provides high efficiency. The geographic leashes can be used in combination with radio propagation model. The main advantage of this paper is that it is efficient in preventing attacks. The drawback of this paper is that its energy efficiency is low, and the global solution is less efficient.

Jakob Eriksson, S. Krishnamurthy, and M. Faloutsos **[2]** say that the security is a key element of any wireless routing protocols. A wireless network can be attacked at all layers of the protocol stack. Particularly very hard attack to counter is the wormhole attack. In the wormhole attack, an attacker, or potentially multiple colluding

attackers, can secretly broadcast data packets between separate locations. This can give a node the feeling that it is the neighbour of a node that is far away. By forging links between far nodes, attackers may be able to operate nodes to send traffic through them, where the attackers can leak, alter or track such traffic. In a wormhole attack, wireless transmissions are recorded at one location and recap at another, creating a virtual link under attacker control. Proposed corrective actions to this attack use tight clock synchronization, specialized hardware, or overhearing, making them challenge to realize in practice. True Link is a timing based remedy to the wormhole attack. The demerit of this paper is that it is an expensive method and it is impossible in low end WSN. The merit of this paper is that it prevents the attack in an efficient manner.

Weichao Wang∗ Aidong Lu† **[3]** says that wormhole attacks in wireless networks can harshly worse the network performance and adjust the security through spoiling the routing protocols and break up the security improvement. This paper develops an approach, Interactive Visualization of Wormholes (IVoW), to audit and expose such attacks in large scale wireless networks in real time. We describe the topological appearance of a network under wormhole attacks through the node position alteration and anticipate the information at dynamically adjusted scales. Here we combined an automatic detection algorithm with corresponding convenient user interactions to handle difficult scenarios that include a huge number of moving nodes and multiple wormhole attackers. Various visual forms have been endorsed to assist the understanding and analysis of the reconstructed network topology and increase the detection rate. The proposed approach can effectively locate the fake neighbour relations without intervening any false alarms. IVoW does not need the wireless nodes to be furnished with any special hardware, thus reducing the additional cost. The proposed approach establishes interactive visualization that can be fortunately integrated with network security mechanisms to greatly increase the intrusion detection capabilities. The merit of this paper is that it avoids overhead and inaccuracy and it is a robustness one. The demerit of this paper is that it does not detect other attacks.

D. Dong, Y. Liu, X. Li, and X. Liao **[4]** say that the wormhole attack is a most harmful threat to wireless ad hoc and sensor networks. The current countermeasures either depend upon specialized hardware devices or make strong expectations on the network in order to pick up the particular warning induced by the wormholes. Those requirements and expectations limit the applications of previous entrance. In this paper, we present our experiment to understand the impact and warning of wormholes and develop distributed detection methods by making as few constraints and expectations as possible. We basically analyze the wormhole problem using a topology procedure and offer an effective distributed approach, which relies solely on network connectivity information. The merit of this paper is a better detection and the demerit of this paper is dynamic topology may reduce efficiency and it is not specific to systems.

Ritesh Maheshwari, Jie Gao and Samir R Das **[5]** suggested that we propose a innovative algorithm for detecting wormhole attacks in wireless networks. This algorithm uses only connectivity information to glance the refused infrastructure in the connectivity graph. The proposed method is fully geographical. This algorithm is self-

governing of wireless communication approach. However, the knowledge gained about approach and node distribution helps to estimate a framework used in this algorithm. We provide a simulation result that shows how the algorithm is able to detect wormhole attacks with 100% detection and 0% false alarm probabilities. Even for very low concentration of networks where the rate of disconnection is very high, the detection probability remains very high. The merit of this paper is that provides very good results (no false alarms and 100% detection) when the network disconnection probability is 0. The demerit of this paper is that it increases the time of detection.

R. Poovendran and L. Lazos **[6]** says that wireless ad hoc networks are imagined to be irregularly arranged in potential environments. Hence, giving safe and continuous communication between the un-tethered network nodes becomes a severe problem. In this paper, we examine the wormhole attack in wireless ad hoc networks. Here we present a graph theoretic framework for planning the wormhole links and derive the necessary constraints for detecting and protecting against wormhole attacks. Based on the structure, we show that any candidate explanation for preventing wormholes should build a sub graph of the geometric graph defined by the radio range of the network nodes. Making use of this structure, we propose a cryptographic tool based on local broadcast keys in order to prevent wormholes. The merit of this paper is that high privacy and the demerit of this paper is that fake user problem may prevail and other attacks may prevail. Based on the survey an idea of the proposed work is explained in the next section.

3. Proposed Architecture

In this section, the idea to detect wormhole attack is presented based on the knowledge gathered on the survey. In the review papers various techniques have been adopted to detect the wormhole attack. In my proposed work there is a centralized and distributed algorithm to detect wormhole. Here we define a threshold value for data transfer. We consider a public key infrastructure for implementing the public key infrastructure. In wireless network we consider each node as a user that has a pair of private and public keys. There is a central authority (CA) in the infrastructure which maintains the identity information of each user. It is a trusted entity which is also responsible for pre-distributing and revoking the key. During the data transfer the sender will request the receiver public key for encrypting the data and the receiver will request the sender public key from CA for decrypting the data. Here when the data transfer takes place the centralized node will monitor whether any innovative packets arrives to a node within the communication range. Each node has a rank and time stamp value. If innovative packets arrive then the rank of each node will be incremented. Next the centralized algorithm will calculate the expected transmission count (ETX) that describes the expected total number of transmission to complete the data transfer. If the ETX value exceeds the threshold value then the centralized algorithm will find the wormhole links. In case if there is no central node to monitor the nodes, then the distributed algorithm takes place. Here the entire network is divided into the cluster. The cluster head will be chosen from each cluster and then assign the role to monitor the nodes. The distributed algorithm will takes place in absence of centralized node. Thus the centralized and distributed algorithm

provides a greater contribution in detecting the wormhole attack.

The overall architecture is presented below, where the centralized algorithm technique is implemented to detect the wormhole attack.

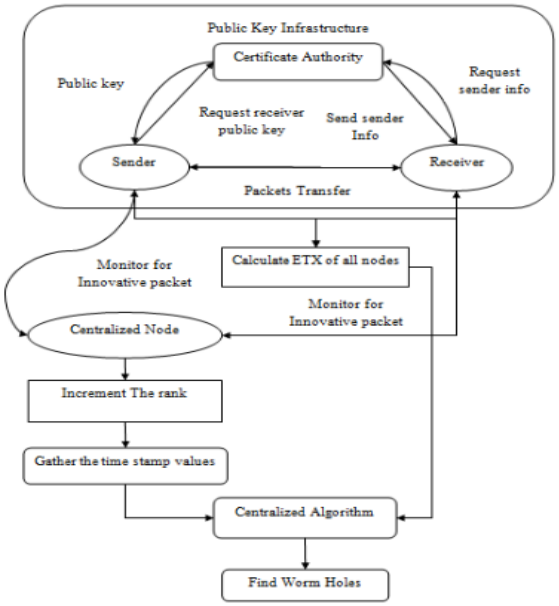

Fig 1. Architecture

3.1 Network Model

In this model, we consider a wireless network with a set of consistent nodes operating network coding protocols. Nodes are coupled via lossy wireless links. For any two pair of nodes say u and v in the network such that the fortunate transmission rate between u and v, p (u, v) > 0, then we say u and v are neighbours. We imagine that ETXs are computed to specify the network topology, and are measured regularly to guide routing functions. Each node receives its own ETXs and its neighbours' ETXs. In the wireless network systems, we imagine that public key infrastructure (PKI) is in position to implement the public key cryptographic method. For the wireless network, we mark all individual nodes as a user who has a pair of public and private keys. The identity and the public key of each user are maintained by the certificate authority (CA), which is a trusted party. If node A needs to securely communicate with node B, A has to demand B's public key from the CA. After the transmission, node B has to demand A's public key from the CA in order to check the message from A. CA is also constrained to pre distribute and call back the key pairs of the nodes. The nodes and the CA together form the PKI, which can assure that no node can fake records from other nodes.

3.2 Detection of Wormhole Attack

In the wormhole attacks, the attackers between different places send packets using a out-of-band channel. This transmission channel is called a wormhole link. The packet loss ratio on the wormhole link is small. The type of the wormhole links can be varying, such as an Ethernet cable, an optical link, or a secured long-range wireless

transmission. When the wormhole attack is triggered, the attackers can catch data packets on both sides, transmit them through the wormhole link and rebroadcast them on the other node. Wormhole attack can have huge impact on wireless network coding systems. Based on different launching time, wormhole attacks can heavily degrade the system performance and can cause each independent node to deal with many non-innovative packets and ruin their resources.

3.3 Role of Central Authority

In this method, we use a centralized algorithm for detecting the wormhole link. For the centralized algorithm, we maintain a central node, which gains an influence to collect information from all nodes in the network, and we run an algorithm based on the rank increment information on the central node. Each node is bounded to report the time. When the rank of the collected packets increases and then generates a report, which includes the information such as the time, the node address, and the rank. Each node provides its reports to the central node via common uncast. The central node chooses an action of rank change, i.e., the rank increases from i to i + 1, and then searches the received reports to find all the related ones. Then we relate the time order of ETXs with the ascending ETX order and then determine the distance between them. If the distance breaks the threshold, we declare then there remains wormhole attack, and then release the warning. At last, we update the bound of the distance for the next detection, in order to make our algorithm a robust one.

3.4 Distributed Approach

In this section, we recognize a practical scenario where the central authority is found to be absence. In this we propose a DAWN, a distributed algorithm to detect wormhole attacks in wireless network coding systems. We will bring accurate analysis on the detection ratio of our algorithm and its resistance against collusions. The main plan of DAWN is that for any two nodes in the neighbourhood, the one with lower ETX is assumed to gain new packets prior than the other one with high probabilities. In other words, the innovative packets are forwarded from low ETX nodes to high ETX nodes with high probabilities. In order to monitor the innovative packets transmission direction, all nodes will work together. Basically, DAWN has two phases on each node for the detection: 1) Report packets and 2) Detect whether any attackers exist.

4. Experimental Results

The following results shows how the presence of wormhole attack is detected during the regular data transmissions in the wireless networks and the way how it is prevented in an efficient manner.This terminal shows that how the nodes are placed in the network. Each node is provided with x,y position. Along with that, the neighbour of each node is calculated. The neighbour node is calculated for the packet transmissions between any two nodes in the network which is as follows.

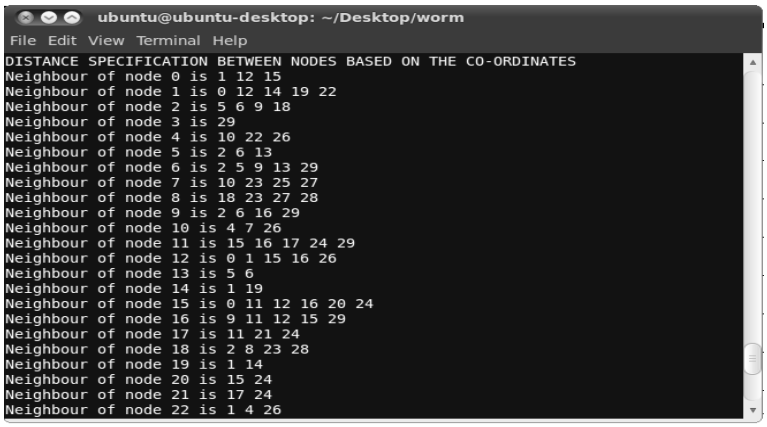

Fig 3. (a) Neighbour node estimation in network

There is a certificate authority which holds the identity information of each node. This certificate authority provides a public key of the receiver to sender in order to safely communicate with each other. In the figure 3(b) the path count is also estimated between source and destination in order to achieve successful data transmission. It also shows the occurrence of wormhole link between any of the nodes in the network as follows.

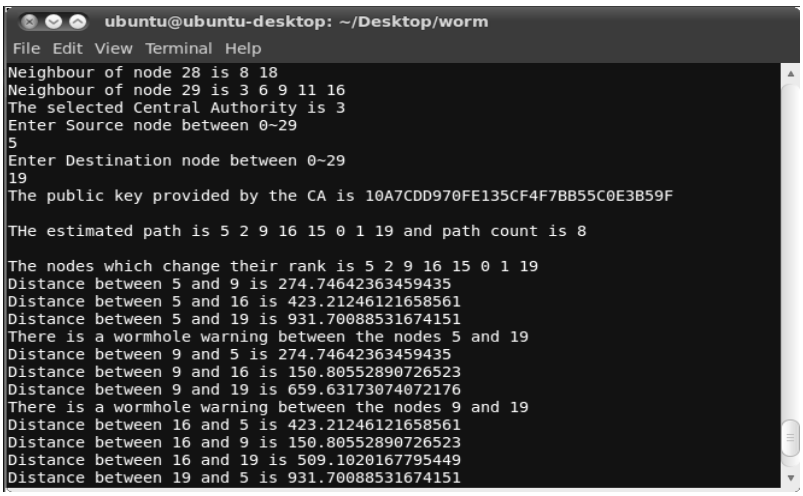

Fig 3. (b) Dtecting wormhole link between nodes

The terminal output shows that the packet is being transmitted from source to destination. Here the red colour node indicates the certificate authority. This shows the animated output. The output is as follows.

The below graph indicates a detection rate. It shows that when the number of nodes in the network increases, the detection rate will increase gradually. The detection rate should be very high in order to efficiently detect the occurrence of wormhole in the wireless network which is described as follows.

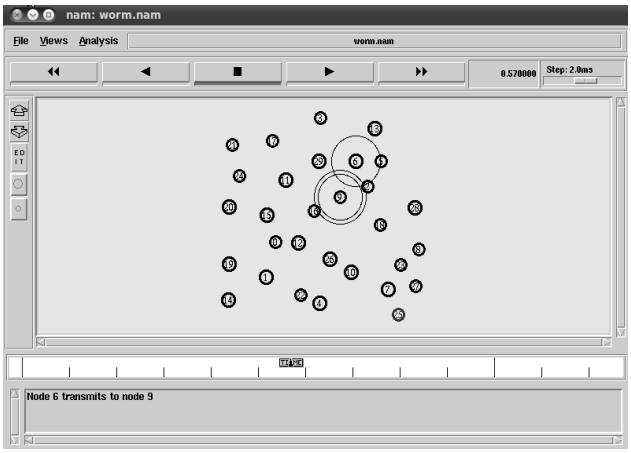

Fig 3. (c) Network animated output

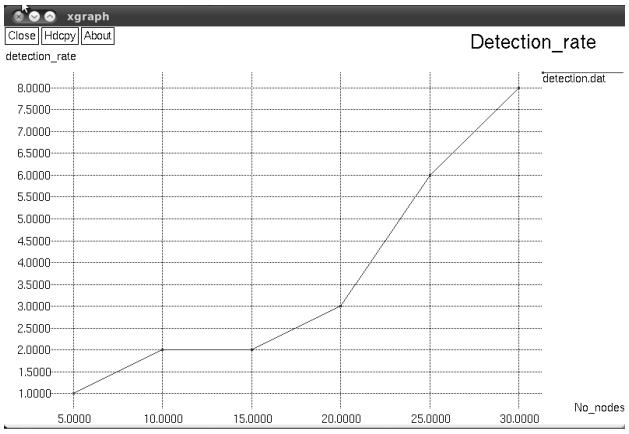

Fig 3. (d) Detection rate of wormhole attacks

5. Conclusion

In this work, we have examined the negative impacts of wormhole attacks on wireless network coding systems. Here we have implemented two algorithms that use the metric ETX to prevent against wormhole attacks. We have implemented a Centralized Algorithm that allows a central node to gather and consider the forwarding behaviours of each node in the network, in order to react immediately when wormhole attack is introduced. We have proven the correctness of the Centralized Algorithm by deriving a lower bound of the deviation in the algorithm.

We have also proposed a Distributed detection Algorithm against Wormhole in wireless Network coding systems, DAWN. DAWN is totally distributed for the nodes in the network, eliminating the limitation of tightly synchronized clock. DAWN is more powerful and thus it suits for wireless sensor network. For both centralized and distributed algorithms, we have used the digital signatures to assure that every report cannot be forged by any attackers.

The simulations have shown that the proposed algorithms can detect the malicious nodes participating in wormhole attack with high successful rate and the algorithm is efficient in terms of computation and communication overhead. My future work is enhanced with the detection of grey hole and black hole attack in wireless network.

References:

[1] Yin-Chun Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in Proc. IEEE 23rd Annu. Joint Conf. IEEE Comput. Commun., Mar. 2003, pp. 1976–1986.

[2] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. IEEE Int. Conf. Netw. Protocols, 2006, pp. 75–84.

[3] Weichao Wang∗ Aidong Lu†, "Interactive wormhole detection in large scale wireless networks," IEEE Symposium on Visual Analytics Science and Technology 2006.

[4] 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.

[5] S. R. D. R. Maheshwari, J. Gao, "Detecting wormhole attacks in wireless networks using connectivity information," in Proc. IEEE 26th Int. Conf Commun., 2007, pp. 107–115.

[6] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," Wireless Netw., vol. 13, no. 1, pp. 27–59, 2007.

[7] W. Wang, B. Bhargava, Y. Lu, and X. Wu, —"Defending against wormhole attacks in mobile ad hoc networks": Research articles, Wireless Commun. Mobile Comput., vol. 6, no. 4, pp. 483–503, Jun. 2006.

[8] B. Nazer and M. Gastpar, —"Compute-and-forward: Harnessing interference through structured codes," IEEE Trans. Inf. Theory, vol.57,no.10,pp.6463–6486,Oct.2011.

[9] Y.-C. Hu, A. Perrig, and D. B. Johnson, —"Wormhole attacks in wireless networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp.370–380,Feb.2006.

[10] W. Wang, B. Bhargava, "Visualization of wormholes in sensor net," in Proc. 3rd ACM Workshop Wireless Security, Oct. 2004, pp. 51–60.