International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 4 No: 3 March 2019

Prevention, Reduction and Recognition of Wormhole Attack by Coordination in the Wireless Adhoc Network

[1]D. Yuvaraj, [2]Shuib Basri
[1]Lecture/Department of CSE, Cihan University, Duhok Kuridsitan Region Iraq. yuvaraj.d@duhokcihan.edu.krd
[2]Software Quality and Quality Assurance (SQ2E) Research Cluster, Univeristi Teknologi Petronas, Perak, Malaysia

Abstract: The adhoc networks are the wireless networks that are briefly established and do not need to be mounted as infrastructure less network. These adhoc networks share a similar wireless medium and lack central coordination that makes them more vulnerable than wired networks to attacks. The intruder senses the packets in terms of bits and tunnels them (possibly selectively) from one location to another location in case of wormhole wireless attack it then sends them back to the network. This kind of wormhole attacks can be a major threat to wireless security systems based on location and adhoc networks per se. To provide strong protection, packet dynamic data can be changed to find a solution over wormhole attack. Wireless election algorithms have chosen the coordinator node to tackle the wormhole attack. The coordinator node's functions are to observe, isolate and prevent further attacks. The simulation experiments were conducted in this context to check the performance in various situations. We have identified from these experimental results that the suggested wireless protocol is adapted to improve the protection of resource-restricted wireless sensor networks.

Keywords: Wireless, Wormhole attack, adhoc, Recognition, defender.

1. INTRODUCTION

A wireless adhoc network or MANET can be a wireless network of a decentralized nature. The network is adhoc because it does not admit pre-existing infrastructure such as wired network routers or wireless network access points. Alternatively, each node participates in routing by transmitting information to different nodes, so determining those nodes forward information is generated dynamically based on the idea of network property and the routing algorithm use. Mobile adhoc network (MANET) is a kind of non-infrastructure adhoc network. It consists of a group of mobile wireless nodes that can communicate with each other. They have dynamic topology, i.e. they can move independently. Whenever necessary, nodes join or leave the network. It is vulnerable to several attacks because the network has no infrastructure [1].

The attack is basically described as a trial to disrupt the network's conventional functionality. The attack also breaches fundamental security goals such as confidentiality, authentication, integrity, availability, and non-repudiation [2]. Two types of attacks are as follows:

- Passive attack-not destroying or disrupting the network, but using the useful information. This type of attack is in breach of confidentiality.
- Captures active attack-it, damages, influences user data. This type of attack is disrupting network operations. Attacks of wormhole and black hole are active attacks.

Wormhole Attack

The attack at Worm Hole is made up of two nodes. The nodes of the attacker that are mainly connected by a link known as the tunnel. The attacker node on one side captures, encapsulates, and transmits the packet from the legitimate node to the other attacker node or malicious node present within the network through tunnel. It consists of one or two malicious nodes and a tunnel between them [3].

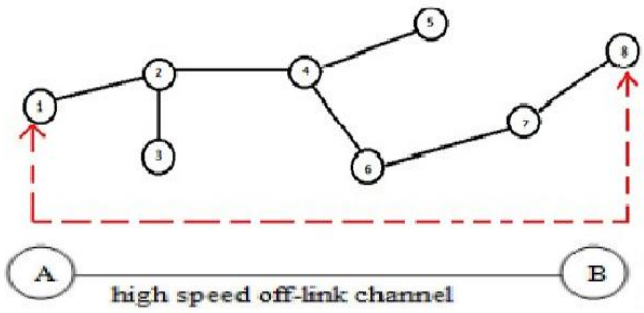

Figure 1. Wormhole Attack

Wormhole nodes are an illusion for the legitimate node of shorter rout than the original route. Fig. 1 shows the wormhole instance. Figure shows two malicious nodes A and B connected by a link, the link can be wired or wireless, the link is referred to as the tunnel, "the tunnel of the wormhole." The attacker nodes communicate with each other through this tunnel [4, 5].

The tunnel is formed through either in-band channel or out-of-band channel or high transmission power. In the Fig. 1 Node3 and Node7 are respectively represented as source and destination. Currently, therefore, the source node3 can transmit the packet to the legitimate neighbor i.e.; node2 can transmit the packet from source to destination during intermediate nodes between node3 and node7 i.e. 2, 6, 5. The legitimate path from node3 to node7, in the absence of malicious nodes, is 3–2–6–5–7, so the number of hops the packet travels is 3 (three).

2. LITERATURE SURVEY

The adhoc wireless sensor networks operate in an extremely hostile atmosphere on low resource constraints of power, battery life, and bandwidth. All the solutions proposed for the wormhole attack do not appear to be monitoring any or all kinds of wormhole attacks. The wormhole attack's success does not depend on cryptographic methodology, but on its attack strength. Solutions based on cryptography dependency are susceptible to attacks of wormhole replay [6, 7]. Throughout the data-forwarding section, however, one-time signature technique is protected in this proposed method routing from different anomalies. Two forms of taxonomy were addressed in this context:

(i) malicious nodes revealing their identity

(ii) which in wormholes does not reveal their identity

They are some limitations in sensors that meant restricted power, limiting bandwidth and economic throwaway devices, that the antenna was supported by the solution for the interference of the attacks and therefore the global positioning system is inadequate for WSN. The packet leashes solution is used to reconcile packet-based wormhole Recognition obstruction (in that the intruder utilizes a lengthy directional antenna). This provision requires time to accomplish the task in wireless sensor networks because it requires additional hardware. Nevertheless, modern research has highlighted the fact that a specific attack, called the wormhole attack, can cause irreparable damage to the routing protocol. In a wireless system, this susceptibility is present and is also likely to exist in adhoc trading systems. Although several efforts have been made to deal with wireless communications wormhole attacks, the solutions offered seem insufficient, requiring further renovation [8, 9]. For these protocols, the analysis of secure forwarding information schemes and Public Key Certificates (PKCs) is required. It should be emphasized that the management of certificates was a profound procedure and that resource-crunch was faced by clients in the brokerage domain. There was a great option for the clients to delegate to the broker the relative duty. It was noted that the broker had sufficient resources and was a Trusted Third Party (TTP). The broker was therefore suitable for the storage and management of PKCs. The latter part of their paper addressed this dilemma, with special emphasis on the management of certificate status, which was the most intricate certificate management function [10].

During packet forwarding, nodes are categorized based on dynamic behaviour. During transmission, misbehaved nodes will be avoided. The forwarding of the packet is based on the reply packet for route forwarding. In this work, r information transmission is highly viable to the breach of protection and vulnerable to issues such as power limitation, information transfer & aggregation, and placement awareness [13, 14].

3. WIRELESS ELECTION ALGORITHM RECOGNITION AND REDUCTION OF WORMHOLE ATTACK

The proposed methodology focuses on selecting a proper leader and using such a leader to mitigate the wormhole attack. Since MANET has dynamic changes in topology, wireless election algorithms must be used to conduct elections. The best work for the leader or coordinators is to find the vulnerability path that is a path with a wormhole tunnel.

As and when the node joins the network, the coordinator must be requested. If the node already has a coordinator, the newly joined node must register it to the coordinator with its configuration details.

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 4 No: 3 March 2019

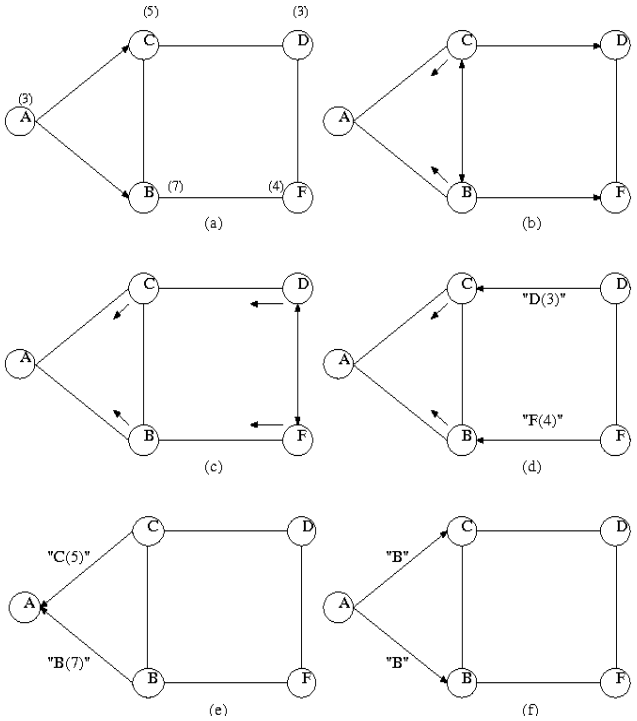

Figure 2. Wireless Election Algorithms

If the MANET has no coordinator, the new node will start the new election. Following the completion of the election as per Fig. 2 The coordinator message will then be sent to all non-coordinator nodes in the network. All other nodes must send the acknowledgment message with the path information from each node to the coordinator by receiving the coordinator message.

Coordinator Algorithms

The algorithms used by the Coordinator to detect and mitigate wormhole attack. Below are the steps in our coordinator algorithm.

Step 1: Perform a successful coordinator selection.

Step 2: Verify that without the coordinator there is no network.

Step 3: The coordinator message will be sent to all the other nodes in the network after the election mechanism.

Step 4: All other nodes must send acknowledgement along with routing path information to reach the coordinator by receiving the coordinator message.

Step 5: Then the work of the coordinator is to examine information about the routing path.

Step 6: If the information on the common path is present.

Step 7: Then coordinators work by sending the empty packet to two tunnel nodes and waiting for recognition.

Step 8: If the coordinator confirms the tunnel, all other nodes in the network will share the routing path.

Step 9: The coordinator will monitor the network continuously.

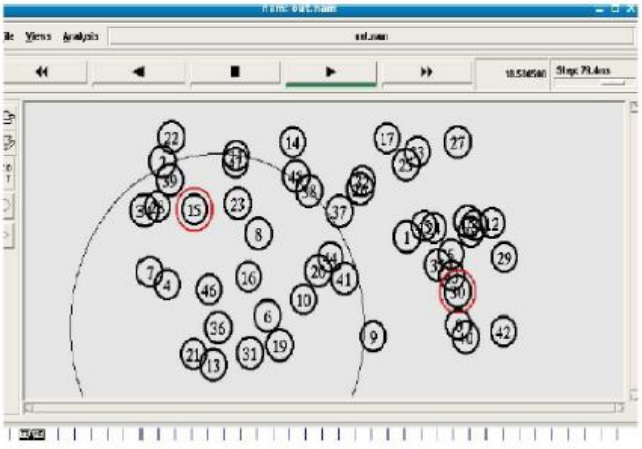

Figure 3. Random Approach Transfer Model

Table 1. Throughput

Nodes	20	40	60	80	100
Normal	83.63	87.12	89.23	89.48	90.02
Attack	28.36	35.57	42.63	47.89	58.32
Prevention	82.31	83.41	88.62	87.45	89.85

4. RESULT AND DISCUSSION

We have implemented the simulation's random approach point transfer model, where a node starts at a random position, waits for the pause time, then moves to a different random position with a speed between 0 m/s and the maximum simulation speed as shown in Fig. 3.

The TUI value that was found to be optimal for networks in previous experiments is about five seconds. The performance metrics are obtained by simulations, networking with a special mobility and connection pattern through ensemble averaging. Metrics such as throughput, Packet Loss By malicious node evaluated the performance of the proposed scheme. Using this method, the coordinator was selected to identify vulnerable tunnels and inform all other nodes about wormhole details to enhance service quality.

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 4 No: 3 March 2019

Table 1 and Fig. 4 Give adhoc network throughput values in normal circumstances, attack scenario and node counts in prevention from 20 to 100 respectively.

Table 2 and Fig. 5 represent adhoc network packet delivery rates in normal situation, attack scenario and node counts from 20 to 100 respectively during prevention.

Table 2. Packet Delivery Rate

Nodes	20	40	60	80	100
Normal	94.57	87.12	96.12	97.23	99.02
Attack	31.26	35.57	42.63	57.89	68.32
Prevention	94.31	86.41	95.62	96.45	98.85

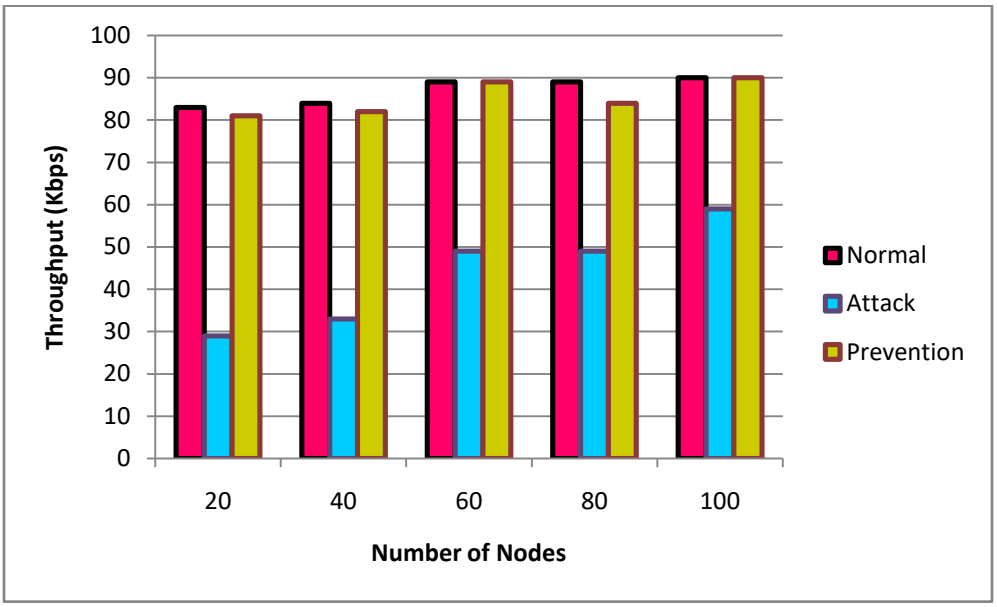

Figure 4. Throughput

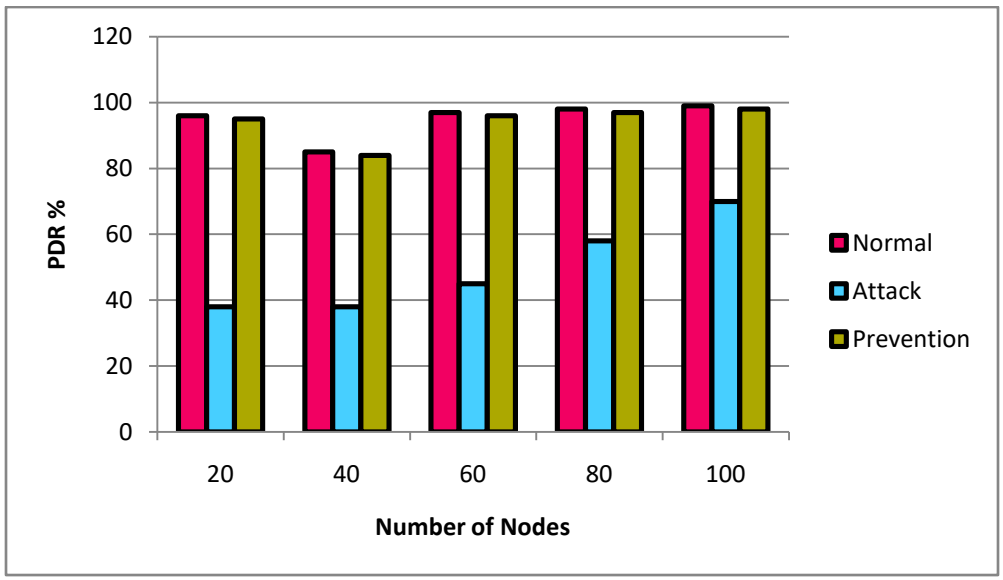

Figure 5. Packet delivery rate

5. CONCLUSION

As adhoc networks and wireless networks in general, computing services are developing rapidly. However, due to its vulnerability to numerous attacks, security concerns still exist when it comes to wireless adhoc networks. Wormhole Recognition in adhoc networks is still considered a complicated task because these types of attacks are carried out by two malicious nodes that cause serious damage to networks and nodes. The solutions proposed in previous literature required specialized hard wares to protect these adhoc networks from wormholes. The aim of this paper is therefore to propose an algorithm that can observe wormholes without any special hard wares. We used the coordinator of wireless election algorithms to identify the attack and path of the wormhole. Once detected, for further prevention of attack, other nodes in the network will be notified of the attack. This algorithm proposal was also verified with optimum results for service quality parameters such as throughput and packet delivery rate.

REFERENCES

[1] Pathan, A.S.K., Lee, H.W. and Hong, C.S., 2006, February, Security in wireless sensor networks: issues and challenges. IEEE 8th International Conference in Advanced Communication Technology 'ICACT 2006, 2, 6- pp, Phoenix Park, South Korea.

[2] Pelechrinis, K., Iliofotou, M. and Krishnamurthy, S.V., Denial of service attacks in wireless networks: The case of jammers, IEEE Communications Surveys & Tutorials, 13(2), 245–257, (2011).

[3] Hu, Y.C., Perrig, A. and Johnson, D.B., Wormhole attacks in wireless networks, IEEE journal on selected areas in communications, 24(2), 370–380, (2006).

[4] Karlof, C. andWagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, adhoc networks, 4(2), 293–315, (2003).

[5] Khalil, I., Bagchi, S. and Shroff, N.B., 2005, June. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In Dependable Systems and Networks, DSN 2005, Proceedings. International Conference on IEEE. Yokohama, Japan, pp. 612–621.

[6] Chiu, H.S. and Lui, K.S, DelPHI: wormhole Detection mechanism for adhoc wireless networks. In Wireless pervasive computing, 2006 1st international symposium on Wireless Pervasive Computing, (pp. 6). IEEE. Phuket, Thailand.

[7] Eriksson, J., Krishnamurthy, S.V. and Faloutsos, M. Truelink: A practical countermeasure to the wormhole attack in wireless networks. In Network Protocols, 2006. ICNP'06, Proceedings of the 14th IEEE International Conference on Network Protocols, ICNP 2006, IEEE, Santa Barbara, California, USA, November. 2006, pp. 75–84.

[8] Maheshwari, R., Gao, J. and Das, S.R., Detecting wormhole attacks in wireless networks using connectivity information, In INFOCOM 2007, 26th IEEE International Conference on Computer Communications. IEEE, Anchorage, Alaska, USA, May 2007, pp. 107–115.

[9] Lazos, L., Poovendran, R., Meadows, C., Syverson, P. and Chang, L, Preventing wormhole attacks on wireless adhoc networks: a graph theoretic approach. In Wireless Communications and Networking Conference, IEEE, New Orleans, LA, USA, March 2005, 2, pp. 1193–1199.

[10] Nait-Abdesselam, F., Bensaou, B. and Taleb, T.,. Detecting and avoiding wormhole attacks in wireless adhoc networks. IEEE Communications Magazine, 46(4), 127–133, (2008).

[11] Qian, L., Song, N. and Li, X., Detecting and locating wormhole attacks in wireless adhoc networks through statistical analysis of multi-path. In Wireless Communications and Networking Conference IEEE, New Orleans, LA, USA 2005, March, 4, pp. 2106–2111.

[12] Song, N., Qian, L. and Li, X.,Wormhole attacks Recognition in wireless adhoc networks: A statistical analysis approach, In Parallel and distributed processing symposium, 2005. Proceedings. 19th IEEE international IEEE. Vancouver, British Columbia, CANADA, April 2005, pp. 8-pp.

[13] Van Tran, P., Hung, L. X., Lee, Y.K., Lee, S. and Lee, H, TTM: An efficient mechanism to detect wormhole attacks in wireless adhoc networks. In Consumer Communications and Networking Conference, CCNC 2007, 4th IEEE Las Vegas, NV, USA, January 2007, pp. 593–598.

[14] Win, K.S., Analysis of detecting wormhole attack in wireless networks. In World Academy of Science, Engineering and Technology, International Journal of Electronics and Communication Engineering, 2(12), (2008).

[15] Znaidi, W., Minier, M. and Babau, J.P., Detecting wormhole attacks in wireless networks using local neighborhood information. In Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC.'08), IEEE Cannes, France, September 2008 pp. 1–5.

