Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/120123

Detection, Prevention and Mitigation of Wormhole Attack in Wireless Adhoc Network by Coordinator

R. Arun Prakash[1,*], *W. R. Salem Jeyaseelan* [2] *and T. Jayasankar*[3]

[1] Department of Computer Science and Engineering, University College of Engineering, Ariyalur, Tamilnadu, India.
[2] Department of Information Technology, J.J. College of Engineering and Technology, Tiruchirappalli, Tamilnadu, India.
[3] Department of ECE, University College of Engineering, Anna University, BIT Campus, Tiruchirappalli,Tamilnadu, India

Received: 18 Nov. 2017, Revised: 17 Dec. 2017, Accepted: 21 Dec. 2017
Published online: 1 Jan. 2018

Abstract: The adhoc networks are the briefly established wireless networks that don't need to be mounted infrastructure it's conjointly called as infrastructure less network. These adhoc networks share a common wireless medium and lack central coordination which makes them more liable to attacks when compared to wired network. In case of wormhole wireless attack, the intruder senses the packets in terms of bits and tunnels them (possibly selectively) from one location to a different location.it then send back them into the network. Such wormhole attacks can be a significant threat against location-based wireless security systems and adhoc networks per se. In an attempt to find the solution over wormhole attack, the dynamic information of the packets can be changed which provides a strong protection. In order to tackle wormhole attack coordinator node has been elected by wireless election algorithms. Functions of the coordinator node are to observe, isolate and prevent any further attacks. In this context, the simulation experiments were carried out to check the performance under different situations. From these experiment results, we have identified that the suggested wireless protocol is adapted for improving the protection of resource constrained wireless sensor networks.

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

1 Introduction

A wireless adhoc network or MANET may be a decentralized kind of wireless network. The network is adhoc since it does not admit a preexisting infrastructure, like routers in wired networks or access points in managed (infrastructure) wireless networks. As an alternative, every node partakes in routing by forwarding information for different nodes, therefore the determination of those nodes forward information is created dynamically on the idea of network property and the routing algorithm in use. Mobile adhoc network (MANET) is a sort of adhoc network which has no infrastructure. It consists of a group of wireless mobile nodes which are capable of communicating with each other. They have dynamic topology i.e. they are free to move independently. Nodes join or leave the network whenever required. As the network has no infrastructure, it is vulnerable to several attacks [1].

Basically, the attack is outlined as a trial to disrupt the conventional functionality of the network. The attack also violates the basic security goals like confidentiality, authentication, integrity, availability, and non-repudiation [2]. There are two types of attack which are as follows:

(1)Passive attack-that does not destroy or disrupt the network, butuses the useful information. This type of attack violates confidentiality.
(2)Active attack-it captures, damages, influences the user data. This type of attack disrupts the operations of the network. Wormhole attack and black hole attacks are active attacks.

1.1 Wormhole Attack

Worm Hole attack consists of two nodes. The attacker nodes that are connected by a link primarily which is known as the tunnel. The attacker node on one side captures the packet from the legitimate node, encapsulates it and transmits through tunnel to the other attacker node or malicious node which arepresent within

[*] Corresponding author e-mail: arunprakashphd@rediffmail.com

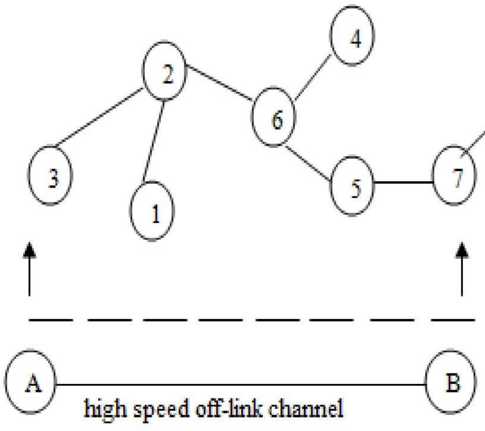

Fig. 1: Wormhole Attack.

the network. It consists of one or two malicious nodes and a tunnel between them [3].

Wormhole nodes form an illusion of shorter rout than the original route for the legitimate node. Fig. 1 shows the instance of wormhole. Figure illustrates two malicious nodes *A* and *B* connected with one another through a link, the link may be wired or wireless, the link is referred as tunnel, “the wormhole tunnel”. Through this tunnel the attacker nodes communicate with each other [4, 5].

The tunnel is formed via in-band channel or by out-of band channel or through high transmission power. In Fig. 1 node3 and node7 are pictured as source and destination respectively. Therefore currently the source node3 can forward the packet to the legitimate neighbor i.e.; node2 during this way intermediate nodes between node3 and node7 i.e., 2, 6, 5 can forward the packet from source to destination. In the absence of malicious nodes, the legitimate path from node3 to node7 are 3–2–6–5–7 therefore number of hops the packet travels is 3 (three).

2 Literature Survey

The adhoc wireless sensor networks functions on low resource constraints of power, battery life, and bandwidth in an extremely hostile atmosphere. All of the proposed solutions to the wormhole attack don’t seem to be surveillance to any or all sorts of wormhole attacks. The success of the wormhole attack is not dependent on cryptographic methodology but depends on its strength of the attack. Solutions which are based on the dependency of the cryptography are susceptible to wormhole replay attacks [6, 7]. However in these proposed method routing from different anomaly is protected throughout the data-forwarding section using the technique of One-Time Signature. In that two forms of taxonomy been addressed: (i) with malicious nodes which reveals their identity and (ii) which doesn’t reveal their identity in wormholes.

They are certain limitation in sensors which meant be power restricted, bandwidth limitation and economic throwaway devices, that the solution for the interference of the attacks supported the antenna and therefore the global positioning system is insufficient for wireless sensor networks. The solution of the packet leashes is used to reconcile the obstruction of packet based wormhole detection (in that the intruder uses a long directional antenna). This provision needs time consuming to achieve the task in wireless sensor networks, as it requires extra hardware. Nevertheless, modern investigations have emphasized the fact that a specific attack, termed as the wormhole attack, is capable of causing irreparable damage to the routing protocol. This susceptibility is present in a wireless system, and it is also likely to exist in adhoc commerce systems. Though several efforts have been made to face the wormhole attacks in the domain of wireless communications, the offered solutions seem to be insufficient, requiring further renovation [8, 9].

The analysis of the secure information of forwarding schemes and However, Public Key Certificates (PKCs) are needed for these protocols. It was to be emphasized that the certificate management was a profound procedure and that clients in the brokerage domain faced resource-crunch. There the excellent option was for the clients to delegate the relative duty to the broker. It was noted that the broker was a Trusted Third Party (TTP) and had sufficient resources. So, the broker was suitable for storing and managing PKCs. The latter part of their document tackled this dilemma, with special emphasis on the certificate status management that was the most intricate function of the certificate management [10].

Nodes are categorized based on dynamic behavior during the packet forwarding. By this misbehaved nodes will be avoided during transmission. The packet forwarding is based on route forwarding reply packet. In this work *r* information forwarding is highly viable to the protection breach and vulnerable to design problems like power limitation, information transfer& aggregation, and placement awareness [13, 14].

3 Detection and mitigation of wormhole attack using Wireless Election Algorithm

The proposed methodology concentrates on selecting a proper leader and mitigating the wormhole attack by using such leader. Since MANET has dynamic topology changes then elections have to be carried out by wireless election algorithm. The best leader or coordinators work is to find the path with the vulnerability that is a path with wormhole tunnel.

As and when the node has joined the network it has to request for the coordinator. If the node has coordinator already then the newly joined node has to register him with his configuration details to the coordinator. If the MANET

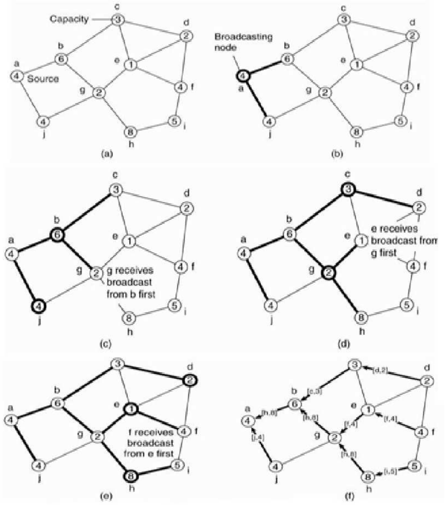
Capacity
Source
Broadcasting node
g receives broadcast from b first
e receives broadcast from g first
f receives broadcast from e first
a
b
c
d
e
f
g
h
i
j
(a)
(b)
(c)
(d)
(e)
(f)

Fig. 2: Wireless Election Algorithms.

doesn't have the coordinator then the new election will be started by the newly joined node.

After the election has been completed as per Fig. 2 then the coordinator message will be forwarded to all the nodes in the network other than coordinator. By receiving coordinator message all other nodes have to send the acknowledgment message with the path information from each node to the coordinator. The coordinator's work is to examine the paths by the acknowledgment message. If there is a single tunnel path stay live means then it has to be isolated and notified to all other nodes in the network.

3.1 Coordinator Algorithms

The Coordinator algorithms used to detection and mitigation of wormhole attack. The steps in our coordinator algorithm are given below.

Step 1: Perform the successful selection of coordinator.
Step 2: Verify that no network without the coordinator.
Step 3: After election mechanism coordinator message will be forwarded to all the other nodes in the network.
Step 4: By receiving coordinator message all the other nodes have to send acknowledgment along with routing path information to reach the coordinator has to be sent to the coordinator.
Step 5: Then the coordinator's work is to examine the routing path information.
Step 6: If there is common path information is present.
Step 7: then coordinators work is to send the empty packet to two nodes of the tunnel and waits for the acknowledgement.
Step 8: If the coordinator confirms the tunnel then that routing path will be shared between all other nodes in the network.

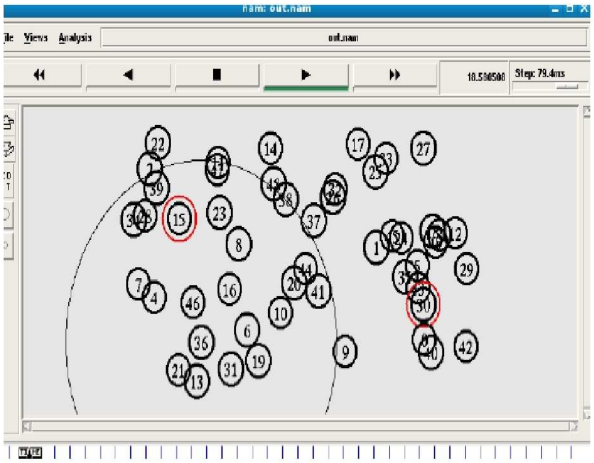

Fig. 3: Random Approach Transfer Model.

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

Step 9: Coordinator will continuously monitor the network.

4 Results and Discussion

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

The TUI value which has been found optimum in previous experiments for networks is about five seconds. The performance metrics are obtained through ensemble averaging by simulations, network with a special mobility and connection pattern. The performance of the proposed scheme has been evaluated by metrics like throughput, Packet Loss By malicious node. The coordinator has been selected by using such to identify vulnerable tunnel and informing the details concerning wormhole to all other nodes to enhance the quality of service.

Table 1 and Fig. 4 give the throughput values of adhoc networks in normal situation, attack scenario and during prevention with node counts from 20 to 100 respectively.

Table 2 and Fig. 5 represent the packet delivery rate values of adhoc networks in normal situation, attack scenario and during prevention with node counts from 20 to 100 respectively.

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

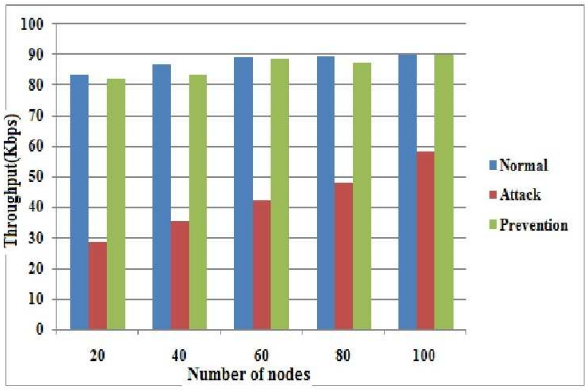

Fig. 4: Throughput.

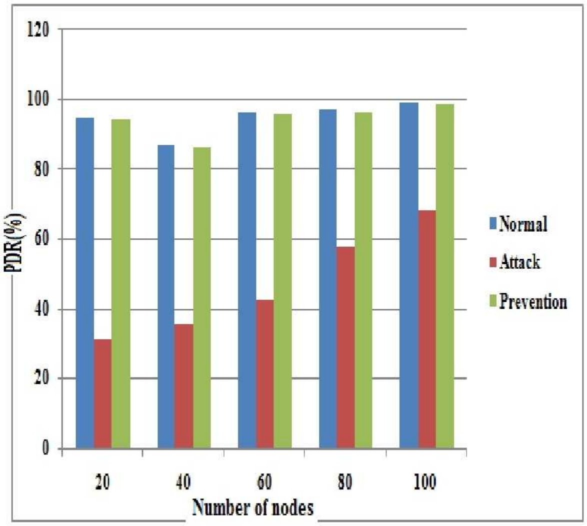

Fig. 5: Packet delivery rate.

5 Conclusion

Computing services are developing rapidly, so are the adhoc networks and wireless networks in general. However, there are still security concerns when it comes to wireless adhoc networks due to its vulnerability to numerous attacks. Wormhole detection in adhoc networks is still considered a complicated task as such types of attacks are executed by two malicious nodes inflicting serious harm to networks and nodes. To protect these adhoc networks from wormholes, the solutions proposed in previous literature needed specialized hard wares. Therefore, the objective of this paper is to propose an algorithm which can observe wormholes without needing any special hard wares. We have used wireless election algorithm coordinator to identify wormhole attack and path. Once detected, other nodes in the network will be notified about the attack for further prevention of attack. This proposal of algorithm was also verified for quality of service parameters such as throughput and packet delivery rate and the results obtained were optimum.

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. and Wagner, 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 detection 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.

R. Arun Prakash received B.Tech. degree in Information Technology from Bharathidasan University, Trichy in 2003, M.Tech. degree in Information Technology at Sathyabama University, Chennai in 2005 and Ph.D. degree in M-Commerce at Anna University Chennai 2016. At present, he is an Assistant Professor in the Computer science and Engineering Department, University College of Engineering, Ariyalur, Anna University, Tamilnadu, India. He is a member of ISTE. He has been a lecturer at graduate and post-graduate level and has participated in a number of International and National level conferences and workshops. He has published around 18 papers in the reputed international journals and more than 10 papers in the international and national conferences and contributed two book chapters. His main interest is currently M-commerce, Mobile computing, image processing and wireless networks.

W. R. Salem Jeyaseelan received Bachelor of Engineering specialized in Electrical and Electronics Engineering from Madurai Kamaraj University, Madurai, India in 2003, Master of Engineering specialized in the field of Computer Science and Engineering from Anna University, Chennai, India in 2007 and Doctor of Philosophy in Information and Communication Engineering from Anna University, India in 2016 . He Published 5 research papers in journals and more than 10 papers in international conferences. He is a life time member of ISTE and has 11 years of experience in teaching and research. Currently he is working as Assistant Professor [SE-G] in Department of Information Technology, J.J. College of Engineering and Technology, Tiruchirappalli-620009, India. His research interests include Adhoc Networks, Wireless Communication, Wireless Networks, Computer Networks and MANET.

T. Jayasankar received the B.E. degree in Electronics and Communication Engineering from Bharathiyar University, Coimbatore in 2001 and M.E. degree at Madurai Kamaraj University,Madurai in 2003 and Ph.D.in Speech Processing at Anna University Chennai 2017. At present, he is an Assistant Professor in the Electronics and Communication Engineering department, University College of Engineering, Anna University, Bharathidasan Institute of Technology Campus, Tiruchirappalli, Tamilnadu, India. He is a member of IEI, ISTE. He has been a lecturer at graduate and post-graduate level and has participated in a number of International and National level conferences and workshops. He has published around 25 papers in the reputed international journals and more than 15 papers in the international and national conferences. His main interest is currently speech synthesis, speech and image processing and wireless networks.