Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Wormhole Attack Detection Techniques In Wireless Mesh Networks

Er. Pinki Tanwar
Assistant Professor, JMIT
Haryana, India

Himani Gupta
Persuing M.Tech , JMIT
Haryana, India

Abstract— Wireless mesh networks (WMNs) have emerged as a promising concept to meet the challenges in next-generation networks providing the ability to configure automatically and re-configure dynamically to maintain the mesh connectivity, which gives the mesh "self-forming" and "self-healing" characteristics. WMN may be dynamic because of changes in both its topology and its membership (i.e nodes frequently join and leave the network). Any security with a static configuration would not suffice. Security of WLAN remains an area of great debate and concern for the foreseeable future. While communicating, various attack occurs like Sinkhole, Blackhole, Denial Of Service, Node Capture, Wormhole attack. The main attack under consideration is Wormhole Attack. In this attack, various attacker nodes establish a direct communication channel b/w themselves & thereby bypass several intermediate nodes through it. The channel to be established can be an out of band high speed communication link. Research objective is to study & analyze various detection methods on the basis of their techniques used & the various hardware requirements.

Keywords— WMN, Wormhole Attack, WGDD , WHOP , Clustered CA

I. INTRODUCTION

The wireless mesh networking has emerged as a promising technology for future broadband wireless access. A wireless mesh network (WMN) consists of mesh nodes which form the backbone of the network. WMN also consist of mesh clients, mesh gateways, mesh routers [2]. The nodes are able to configure automatically and re-configure dynamically to maintain the mesh connectivity which gives the mesh "self-forming" and "self-healing" characteristics. The need for centralized management is removed due to this self sufficient relationship. Intelligent routing allow mesh nodes to route data packets for nodes that may not be within direct wireless range of each other. Especially for backhaul communication, this has a big advantage in terms of network reliability over traditional single hop networks.

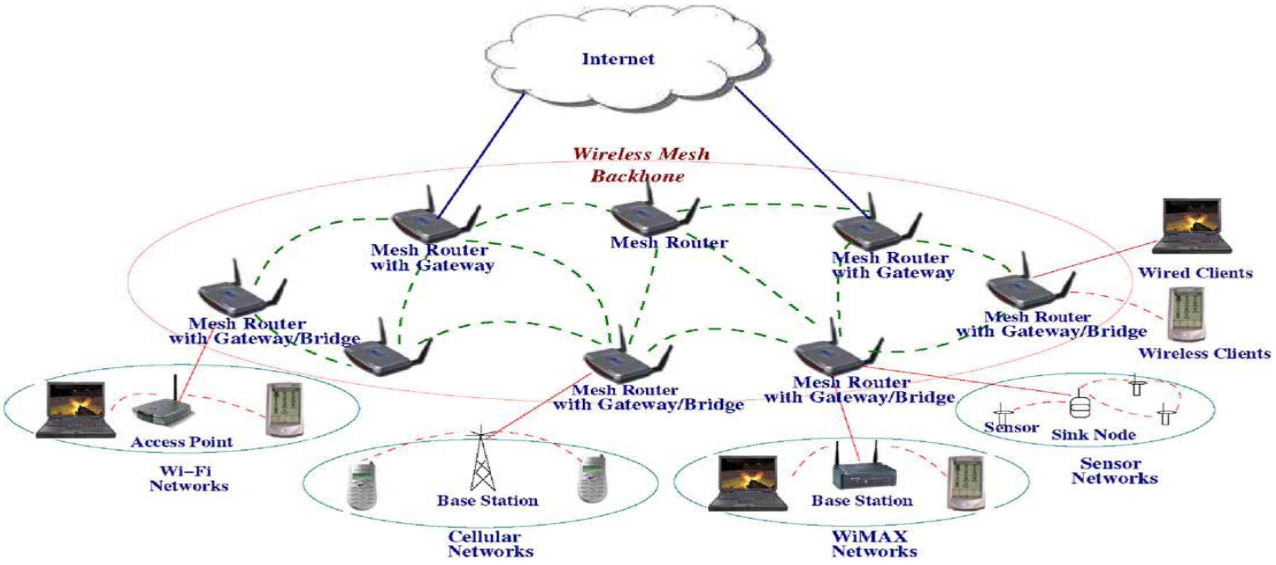

Fig. 1: EXAMPLE OF WMN

A wireless mesh node consists of a wireless router and an antenna. It could be installed indoors or in a weather-proof enclosure outdoors. The antenna could be the standard indoor omni-directional antenna or it could be an externally mounted omni directional or directional antenna. It communicated with end clients and mesh nodes.

]

In wireless mesh networks (WMNs) wireless mesh routers form densely interconnected multi-hop topologies. For local communication and routing to a wired access network the routers automatically configure a wireless broadband backbone. Three kinds of wireless mesh networks can be identified.

1) In infrastructure WMNs mesh routers form a network offering services to client users. The network thus has self-healing characteristics .
2) Client WMNs are ad-hoc networks formed by clients amongst themselves. None of the dedicated routers or infrastructure exists, so that the clients have to be self-configuring and act as routers for the traffic in the client WMN
3) Hybrid WMNs combine the advantages of the two other WMNs.

II. SECURITY CHALLENGES IN WMN

As we look at Wi-Fi security, it is dangerous to focus only on one mechanism of security, such as data encryption, or making decisions on defending against a certain type of attack. Also, it is wrong to ignore security weaknesses just because they have low consequences. The main difficulty in establishing a wireless network is being able to support effective security so that users can access network without fear of leaking mission-critical data through the airwaves in or near the perimeter of office building.

Why don’t most people enable security by choice? This is an important question that has a simple answer. An 802.11b network, for example, with the best possible range and signal, has a maximum throughput of 11 Mpbs. Today people are finding wired 100 Mpbs LANs too congested for transferring files and other large objects over the network. When you enable security on a wireless device, there is a certain degree of overhead that reduces the overall speed of your connection because it is effectively encrypting your network traffic on one end and decrypting it on another end. While the computer processes this information quite quickly, it cuts into your overall speed.

The security challenges of WMNs are rooted from their topology features. By analyzing the characteristics of WMNs and comparing them with other networking technologies , the authors show that the new security challenges are mainly due to the multihop wireless communications and by the fact that the nodes are not physically protected. Multihopping is indispensable for WMNs to extend the coverage of current wireless networks and to provide non-line-of-sight (NLOS) connectivity among users. Multihopping delays the detection and provides treatment for them , makes it very critical and may lead to severe unfairness between the nodes .

In addition, nodes rely on each other to communicate, and thus the cooperation of node is indispensable. While the use of wireless links renders a mesh network susceptible to attacks, the physical exposure of the nodes allows them to keep track of these devices.

Other specific challenges for WMNs include:

1) WMN may be dynamic because of changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Any security with a static configuration would not suffice
2) In WMNs, mesh routers and mesh clients hold significantly different characteristics such as mobility and power constraints. As a result, the same security solution may not work for both mesh routers and mesh clients.
3) There are also issues introduced by MN belonging to different authorities, such as selfish and greedy behavior, and trust management.

III. WMN SECURITY ATTACKS

Any attempt to destroy ,expose ,alter or gain unauthorized use of an asset are generally known as security attacks.

1) Denial of service attack: DoS attacks are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internet access this type of attacks are common in the network.

2) Node capture attack: An attacker physically captures nodes and compromises them such that readings sensed by compromised nodes are manipulated or compromised. In addition, they may also attempt to extract essential cryptographic keys (e.g., a group key) from wireless nodes that are used to protect communications in the very most wireless networks.

3) Selective forwarding: In selective forwarding type of attack, attacker nodes simply drop certain messages instead of moving forward it . Once an attacker node cherry picks the messages, it keeps on reduces the latency and deceives the neighbouring nodes that they are on a shorter route. Effectiveness depends on following two factors
   a) The percentage of messages it drops.
   b) Location of the malicious node, the more closer it is, the more traffic it will attract. When selective forwarder drops more messages and forwards few, it regains its remaining energy enough powerful to trick the neighbouring nodes.

4) Routing attack: Routing attacks in WMNs could be:
   a) Wormhole attack – In this type of attack,malicious nodes establish a direct communication channel b/w themselves & thereby bypass several intermediate nodes through it.The channel which is to be established can be an out of band high speed communication link.This communication link is referred to as Wormhole.
   b) Routing table overflow attack - an attacker attempts to create routes to nonexistent nodes with intention to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to a resource exhaustion.
   c) Sinkhole Black hole/ attack - a malicious node uses the routing protocol to make it advertise itself as having the shortest path to the other node. In this situation, the malicious node advertises itself to a node that it wants.

IV. WORMHOLE BASED ATTACK

While communicating, various attack occurs in wireless mesh networks like Sinkhole, Blackhole, Denial Of Service, Node Capture, Sybil, Wormhole attack. The main attack under consideration is "Wormhole Attack". In wormhole attack, In Wormhole attack, when both the source and destination are going to start communicate, intruders activate a wormhole based link, which is a high bandwidth wireless link and listen to the communication done by communicating agents with the help of wormhole link.

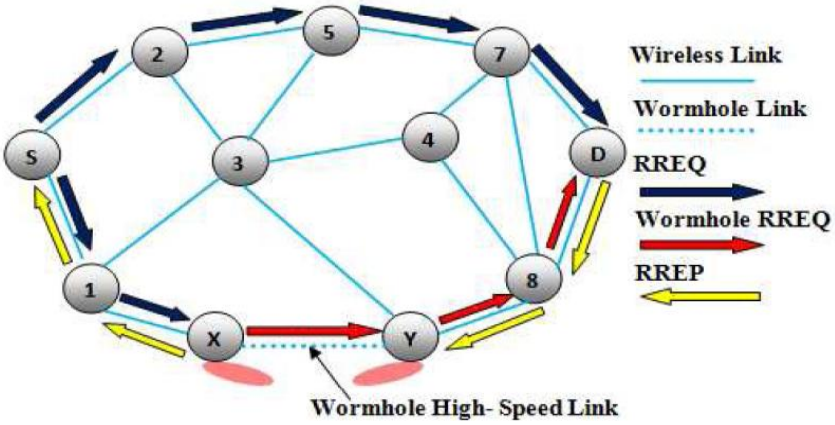

Fig. 2: Wormhole Attack

In the above Fig. 2, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The source node "S" when initiate the RREQ message to find the route to node "D" destination node. The immediate neighbour node of source node "S", namely "2" and "1" forwards the RREQ message to their respective neighbour "5" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbour node "8", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-1-8-D> for destination. It results in ignoring the RREQ that arrived at a later time and thus invalidates the legitimate route <S-2-5-7-D>. The communication done by <S-1-8-D> is thereby listened by the wormhole nodes "X" and "Y". So the wormhole nodes and their high speed link pose a major security threat to the network.

V. CHARACTERISTICS OF SECURITY SOLUTION FOR WMN

Security of WLAN remains an area of great debate and concern for the foreseeable future.The problem with most wireless LANs is that security is often considered optional and is turned off by default We here presents the characteristics solution that a security mechanism for WMN should have, in order to successfully prevent, detect and counteract these attacks. We only presents the various characteristics that differentiate WMN security mechanisms from existing security mechanisms for wired and wireless networks.

1) In wired networks, the security services of data confidentiality and data integrity are generally provided on a per link basis (between two devices). This is based on the assumption that the end devices are secure. However, the WMN nodes may resort to the selfish and malicious behaviour. To counteract the selfish and malicious behaviour of the intermediate hop nodes, the WMN must provide the end-to-end services of data confidentiality and data integrity, in addition to the security services on per link basis.

2) The trust establishment mechanism should be robust against internal selfish and malicious behaviour. Note that they are part of WMN therefore the conventional authentication mechanisms based on cryptographic primitives may not be effective against the internal misbehaviour.

3) Wireless mesh networks are self administered networks and lack the centralized administration authority which can respond to the network issues. Therefore, the attack and anomaly detection mechanisms for wireless mesh

networks should be self sufficient and must not be dependent on the administrator to verify the possible attacks and their anomaly alerts.

VI. LITERATURE SURVEY

The various approaches used for the prevention and detection of wormhole attack in Wireless Mesh Networks is described below:

A. Wormhole Geographic Distributed Detection

An algorithm for the distributed detection of wormhole attack is provided by Yurong Xu in 2007 [1] called wormhole geographic distributed detection (WGDD). WGDD algorithm detects the wormhole attack based on the damage caused by them and the parameter it used is hop count. On the basis of hop count, it again constructs their mapping details in each node and finally it exploits diameter feature to detect distortions caused by attacker nodes. This algorithm is mainly effective in finding the exact location of the wormholes.

B. Neighbour Discovery & Link Verification

This process provided by V.S.Shankar Sriram, Ashish Pratap Singh [2] in 2009 is used to build the data structure of the first hop neighbours of each Access point and the neighbours of each neighbour. The data structure is used in local monitoring to detect malicious AP and in local response to isolate these AP which are pretending to be false neighbours. A neighbour of X is any AP that lies within the transmission range of X. As soon as AP, say A, is deployed in the field, it does a one-hop broadcast of a HELLO message. Any AP, say B, that hears the message, sends back a reply to A. A accepts all the replies that arrive within a timeout. For each reply, A adds the responder to its neighbour list. When B hears the broadcast, it stores RA. Hence, at the end of this neighbour discovery process, each AP has a list of its direct neighbours and the neighbours of each of its direct neighbours. This process is performed only once in the lifetime of an AP and is assumed to be secure. Link verification starts immediately after the completion of neighbour discovery. It uses a collaborative detection strategy, where an AP monitors the traffic going in and out of its neighbours.

C. Threshold authorization with Clustered CA

A threshold authorization model [3] provided by Divya Bansal in 2010 with Clustered CA would stand midway between the two considered extreme models: It enforces a security policy that requires a K members' collaborative decision for issuing, renewing and revocation of certificates. Hence, the decision making is neither fully centralized nor fully distributed .In fact, a threshold authorization scheme employment in a WMN would ensure the distribution of trust among the network members, without relying on transitive trust. This way, the authorization privileges are neither restricted to one certification authority, however, they are not fully distributed in a way to allow one member to grant a valid certificate to a new user.

D. Hop Count & Time Delay

The author Pushpendra Niranjan, Prashant Srivastava in 2012 implements a new method [4] which detects the attacker nodes and works without any modification of protocol & uses a hop-count and time delay analysis from the viewpoint of users without any special environmental assumptions. The work is simulated using OPNET. It provides good performance for detecting tunneling attacks & it detects 75 percent of attackers within five minutes, In addition, since we only select part of the searched routes for multi-path transmission, the probability that malicious nodes can occupy the route are further reduced.

E.Hybridized WHOP with time synchronization

The author Huaiyu Wen in 2013 proposed approach [6] which provides efficient results to secure data packet transmission and reduce the process delay time while not use of any expensive hardware. The author work with DSR routing protocol that simulates the behavior of wormhole attack using network simulator NS-2.

F. Using Directional Neighbour List

The author Priti Gupta, suveg moudgil in 2014 proposed [7] a wormhole detection algorithm for wireless mesh networks which detect the wormholes by calculating neighbour list and directional neighbour list of the source node. The main goal of the algorithm is that it can provide approximate location of nodes and effect of wormhole attack on all nodes which is useful in implementing countermeasures. The performance evaluation is done by varying no. of wormholes in the network. The aim is to propose scheme for wormhole detection and performance evaluation.

VII. OUTLINE OF THE VARIOUS WORMHOLE DETECTION METHODS

In the following Table, contains all wormhole detection methods that are explained previously and also contains the requirements of each method, their features, on which the particular method is based, their hardware needs along with the overheads. synchronization which plays an important role.The table containing all these is shown below.

METHOD	AUTHOR & YEAR	BASED ON	FEATURES	H/W NEDDS & OVERHEAD	LOCALIZATION & CLOCK SYNCHRONIZATION
WGDD (Wormhole Geographic Distribution Detection)	Yurong Xu In 2007	Detecting Network Disorder	Makes use of bootstrap node calculates local map from hop coordinates	Hardware device is needed to calculate the mapping details in each node More overhead	Localization information is needed as it uses diameter in local map No need of clock synchronization
Neighbour Discovery & Link Verification	V.S.Shankar Sriram, Ashish Pratap Singh, G.Sahoo in 2009	Shared information b/w communication access points	Make use of the data structure of hop neighbor Reduced cost Prevent rouge access points from behaving as false neighbours	No extra devices or H/W is needed Overhead is relatively lower	No need of clock synchronization & localization information
Threshold authrization with Clustered CA	Divya Bansal, Sanjeev Sofat in 2010	Secret Key Sharing schemes	Network performance increases with no. of guard nodes Distributed Authorization	No need of Hardware device Low overhead	No need of Localization & clock synchronization
Hop Count & Time Delay	Pushpendra Niranjan, Prashant Srivastava in 2012	ID based Cryptograpjic methods	Works without modification of protocol There's no special environment assumptions	No need of Hardware Still there's high overhead due to use of digital signatures	Localization & synchronization information both not applicable to this type of method
Hybridized WHOP with time synchronizat-ion	Neha Jain,Ashish kr. Srivastava in 2013	Secure Data packet transmission using hound packet	Detects both type of in band & out band wormhole attack Reduces process delay time	No Hardware needed Overhead gets relatively increased	Clock synchronization is there but no need of localized information
Directional Neighbour List	Priti Gupta, Suveg Moudgil in 2014	Directional Antennas	Provides approximate location of nodes Make Efficient use of energy & bandwidth	Extra hardware device is needed for evaluation Overhead gets increased	Localization information is needed to locate but clock synchronization not applicable.

VIII. CONCLUSION

In this paper we reviewed the various detection mechanisms against wormhole attacks in wireless mesh networks. We have also done the qualitative comparison of all the detection techniques & thus a significant amount of work has been done on solving this problem. We can't conclude that only one solution is quite applicable to all the situations. So there are choice of solutions available like hybridized WHOP which detects both in band and out band attack but overhead is getting relatively increased ,while with the clustered CA authorization, performance increases with guard nodes and overhead gets lower. Thus increasing security using various hardware may lead to better performance, but can be sometimes costly, which may affect other networks .

IX. REFERENCES

[1] Yurong Xu, Guanling Chen, James Ford and Fillia Makedon, 2007 "Detecting wormhole attacks in wireless sensor networks" International Federation for Information Processing proceedings on critical infrastructure protection, volume 253, pp. 267-279

[2] V.S. Shankar Sriram, Ashish Pratap Singh, G.Sahoo, International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, May 2009

[3] Divya Bansal and Sanjeev Sofat , Department of Computer Science & Engineering, PEC University of Technology, Chandigarh, Int. J. of Advanced Networking and Applications Volume: 01, Issue: 06, Pages: 387-392 (2010)

[4] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap Information Technology, LNCT (RGPV) Bhopal, India , International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012, ISSN 2250-3153

[5] Huaiyu Wen and Guangchun Luo , Journal of Information & Computational Science 10:14 (2013) 4461–4476, September 20, 2013

[6] Priti Gupta,Suveg Moudgil, CSE Department, KUK University,Haryana ,India, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014,ISSN 0975-9646

[7] Nadher M. A. Al_Safwani, Suhaidi Hassan, and Mohammed M. Kadhum, Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011,8-9 June, 2011 Bandung, Indonesia.

[8] Poonam Dabas1, Prateek Thakral, Volume 3, Issue 3,March 2013, ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[9] M. Jain, H. Kandwa1, "A Survey on Complex Wormhole Attack in Wireless Ad-Hoc Network," in Advances in Computing, Control & Telecommunication Technologies, pp. 555-558, 2009

[10] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[11] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.

[12] L. Lazos, and R. Poovendran, "SeRLoc: Secure Range- Independent Localization for Wireless Sensor Networks," in ACM WiSE'04, New York, NY, USA, pp. 73–100, October 2004.

[13] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, ad hoc mobile wireless networks :principles, protocols, and applications, 1st ed.: Auerbach Publications, 2007.

[14] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[15] Monika Department of computer science, Monika / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4516-4522