

Methodology for Securing Wireless LANs Against Wormhole Attack

V.S.Shankar Sriram¹, Ashish Pratap Singh², G.Sahoo³

^{1,3}Birla Institute of Technology- Mesra/Dept. of Information Technology, Ranchi, India

Email: sriram@bitmesra.ac.in, drgsahoo@yahoo.com

Abstract-- Wormhole attacks enable an attacker with limited Resources and no cryptographic material to wreak havoc on wireless networks. Initial research focused that this attack is possible only on Adhoc networks, but in present Scenario wormhole attack is possible on infrastructure based wireless LANs also. We propose architecture and analyze the possibility of wormhole attack along with a countermeasure to avoid such an attack. The proposed mechanism involves the shared information between communicating Access Points to prevent Rouge Access Points from masquerading as false neighbors. Our defense greatly diminishes the threat of wormhole attacks and requires no location information or clock synchronization.

Keywords—Wireless Network, Access Point (AP), wormhole attack, Rouge Access Point (RAP).

I. INTRODUCTION

Wireless networks are promising platforms for a variety of application areas in both military and civilian domains. These networks are especially attractive for scenarios where it is infeasible or expensive to deploy significant networking infrastructure. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. These attacks could involve eavesdropping, message tampering, or identity spoofing, which have been addressed by customized cryptographic primitives in the wired domain. Routing in wireless networks is an especially hard task to accomplish securely, robustly and efficiently. Many proposed routing protocols are focused on energy, and provide no protection against an adversary. Some secure routing protocols also have been proposed. However, due to the unpredictability of wireless networks, it is hard to detect behavior anomalies in route discovery. In particular, proposed routing protocols cannot prevent [1] wormhole attacks. Initially all proposed protocol to prevent wormhole attack focused on Ad-hoc network only, but in present scenario wormhole attack is possible in Infrastructure mode also by using two rouge access point and high quality, low-latency link. A Rouge Access Point is a Wi-Fi Access Point which is setup by an attacker for the purpose of sniffing wireless network traffic. In a possible wormhole attack for infrastructure mode, an attacker introduces two Rouge access point into a wireless back-haul network and connects them with a high quality, low-latency link. Routing messages received by one wormhole endpoint are retransmitted at the other

endpoint. Attackers can exploit wormholes to build bogus route information, selectively drop packets, and create routing loops to waste the energy of network. We propose a hybrid architecture and possible severe security attack, called the wormhole attack, in the context of proposed architecture.

The rest of the paper is organized as follows: Section II describes Worm-hole attacks, Section III focuses on the related work, Section IV describes the proposed Methodology, Section V addresses Detection strategy and the algorithm for securing the network against wormhole attacks and the final section concludes the paper.

II. WORMHOLE ATTACKS

This section introduces wormhole attacks and explores the possibility of wormhole attack in infrastructure nodes. First let us see how a wormhole attack is done in Adhoc networks. The wormhole attack can prevent two nodes from discovering legitimate routes greater than two hops away and thus disrupt network functionality. A successful attack may result in a disruption or breakdown of a network. Figure-1 shows a typical wormhole attack. The attacker replays packets received by X at node Y, and vice versa. If it would normally take several hops for a packet to traverse from a location near X to a location near Y, packets transmitted near X traveling through the wormhole will arrive at Y before packets traveling through multiple hops in the network. The attacker can make A and B believe they are neighbors by forwarding routing messages, and then selectively drop data messages to disrupt communications between A and B.

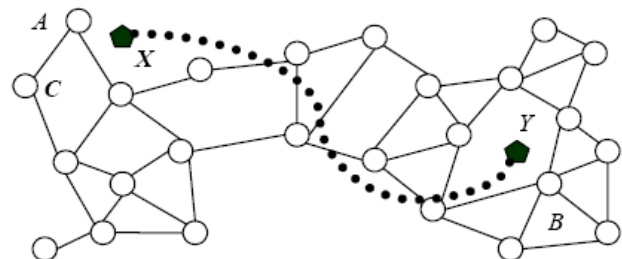


Figure 1. Wormhole attack.

Figure 2 shows a typical scenario of a possible worm hole attack in the Infrastructure WLANs. A Rouge Access point captures packets from one location in the network, and “tunnels” them to another at a distant point, which

replays them locally. [2, 3, 4] The tunnel can be established in many different ways, e.g., through an out-of-band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. This makes the tunneled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multi-hop routes. This creates the illusion that the two end points of the tunnel are very close to each other.

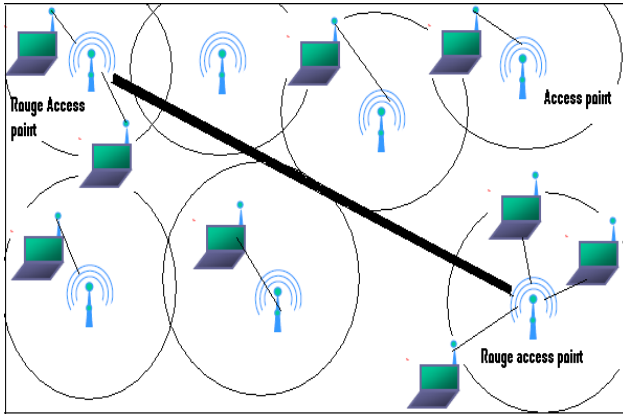


Figure 2. Worm hole attack in Infrastructure mode WLANs

. The adversary controls Rouge access points X and Y and connects them through a low-latency link. Finally, it is worth noting that the wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network.

III. RELATED WORK

A lot of research has been done in exploring wormhole attacks and a variety of counter measures to overcome the same has been proposed. The wormhole attack in wireless networks was independently introduced by Dahill [5], Papadimitratos [6], and Hu [7]. Initial proposals to thwart wormhole attacks suggest using secure modulation of bits over the wireless channel that can be demodulated only by authorized nodes. This only defends against outside attackers who do not possess cryptographic keys. A similar approach called RF watermarking [8] modulates the radio waveform in a specific pattern and any change to the pattern is used as the trigger for detection. This mechanism will fail to prevent a wormhole if the waveform is accurately captured at the receiving end of the wormhole and exactly replicated at the transmitting end.

Hu et al. [7] introduced the concept of geographical and temporal packet leases for detecting wormholes. They define a leash to be any added information to the packet for the purpose of defending against the wormhole. The geographical leash sensor confirms that the recipient of the packet is within a certain distance from the sender. They require each node to know its own location and require all the nodes to have loosely synchronized clocks. The temporal leases ensure that the packet has an upper bound on its lifetime, which restricts the maximum travel Distance. They require that all nodes have tightly synchronized clocks. An implicit assumption

is that packet processing, sending, and receiving delays are negligible. Both geographical and temporal leases need to add authentication data to each packet to protect the leash, which add processing and communication overhead. In addition, a large amount of storage is needed at each node since a hash tree based authentication scheme (Merkle hash trees) is used.

Capkun et al. [9] presented SECTOR, a set of mechanisms for the secure verification of the time of encounters between nodes in multi-hop wireless networks. They show how to detect wormhole attacks without requiring any clock synchronization through the use of MAD (Mutual Authentication with Distance-Bounding). Each node u estimates the distance to another node v by sending it a one bit challenge, which node v responds to instantaneously. Using the time of flight, node u detects if node v is a neighbor or not. The approach uses special hardware for the challenge request-response and accurate time measurements. Neither of the above two techniques nullifies the capacity of the compromised nodes from launching attacks in the future.

Hu and Evans [10] used directional antennas [11,12] to prevent wormhole attacks. To thwart the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors. Neighbor lists are built in a secure manner by using the direction in which a signal is heard from a neighbor with the assumption that the antennas on all the nodes are aligned.

However, it only partially mitigates the wormhole problem. Specifically, it only prevents the kind of wormhole attacks in which malicious nodes try to deceive two nodes into believing that they are neighbors. Moreover, the requirement of directional antennas on all nodes may be infeasible for certain deployments. Finally, the protocol may degrade the connectivity of the network by rejecting legitimate neighbors in their conservative approach to prevent wormholes from materializing.

Till now there is no concrete research which addresses the possibility of a worm hole attack in Infrastructure WLANs. As a core we would like to expose this fact that there is a possibility of a wormhole attack in Infrastructure WLANs. This type of attack uses a set of rouge access points and a base channel of low latency to achieve this attack. There are some tools/software to identify a rouge access points. The two most popular tools of choice are Netstumbler and Kismet. These tools work by attempting to identify the wireless networks within range, and can be used to detect the presence of an access point which is unauthorized. The fundamental difference between the two is the manner in which they work; Netstumbler is termed as an active sniffer whereas Kismet is a passive sniffer.

Netstumbler:- Netstumbler is a piece of software that works on the Windows platform. It works by sending an 802.11 Probe request to a broadcast address, upon receiving this packet all access points within the signal issue a probe response containing their network configuration information that includes their SSID and whether WEP is enabled or not. Furthermore, it can also be integrated with a GPS unit that allows the position of

discovered access points to put onto a map for easier consumption.

Kismet:- Kismet is a passive sniffer with the ability of detecting 802.11 packets for the presence of a WLAN. It identifies networks by collecting packets and identifying their name. It is also capable of detecting hidden networks unlike Netstumbler. The use of Kismet, however, may be deemed as illegal unless prior authorization has been provided from owners of the access points, whose traffic is being captured. Although, if the scan is in an area where multiple access points are owned by numerous entities then getting authorization may not be feasible.

Identifying a rouge access point is a little difficult one, because if there are multiple rouge access points the tool may fail to identify some of them. As of now identifying a wormhole in Infrastructure WLANs is still under cover. We explore this and propose a methodology which can not only identify a rouge access point but also prevent Infrastructure LANs from wormhole attacks.

IV. PROPOSED METHODOLOGY

For the purpose of explaining our methodology we take an example of a WLAN as in Figure 3. To achieve a real Wireless network we need to provide a wireless backhaul between the access points. In our architecture we have one access point connected to the corporate network (i.e) the wired network using a wired backhaul, the access points that cover the entire area are installed in such a way that they have a wireless backhaul and are wirelessly connected to the nearby access points.

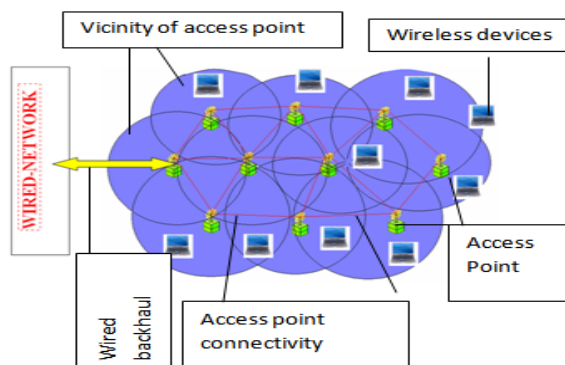


Figure 3. Sample architecture

We also assume that the wireless devices that are a part of our WLAN can roam across the network and have a single sign on or one point authentication. Our proposed work involves two modules, namely:-

1) Neighbors Discovery, 2) Link verification these two process work simultaneously to detect and prevent wormhole in our architecture.

A. System assumption

We assume that the communication links are bidirectional which means that if a node A can hear node B then B can

hear A. We assume that a finite amount of time is required from a node's deployment for it to be compromised. We further assume that no external or internal Rouge Access points exist before the completion of the first- and second-hop neighbor discovery. External RAP is AP that is added to network by an attackers for purpose of creating wormhole and the internal RAP are existing AP in the network which are used for creating wormhole. Route changes due to Access point failures is not permitted that is network is completely functional and all the access points are operational.

B. Neighbors Discovery

This process is used to build the data structure of the first-hop neighbors of each Access point and the neighbors of each neighbor. 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 neighbors. A neighbor of X (AP), 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 neighbor list RA (Responder of Access point). Then, A does a one-hop broadcast of a message containing the list RA. When B hears the broadcast, it stores RA. Hence, at the end of this neighbor discovery process, each AP has a list of its direct neighbors and the neighbors of each of its direct neighbors. This process is performed only once in the lifetime of an AP and is assumed to be secure. Henceforth, a AP will not accept a packet from a node that is not a neighbor, nor forward to a AP that is not a Neighbor. Also, second-hop neighbor information is used to determine if a forwarded packet comes from a neighbor of the forwarder. If a node C receives a packet forwarded by B purporting to come from A in the previous hop, C discards the packet if A is not a second-hop neighbor. Finally, A activates local monitoring immediately after building its first and second-hop neighbor lists.

C. Link verification

This module detects the wormhole attack and diagnoses the malicious AP involved in launching it. Link verification starts immediately after the completion of neighbor discovery. It uses a collaborative detection strategy, where an AP monitors the traffic going in and out of its neighbors. For an AP, say V, to be able to monitor an AP say, M, V must be a neighbor of both M and the previous hop from M, say B. If this is satisfied, we call V the Verifier AP of M over the link from B to M. This implies that V is the Verifier AP for its entire outgoing links. For example, in Figure 4, Access points M, N, and X are the Verifier AP of A over the link from X to A. Information for each packet sent from X to A is saved in a watch buffer at each Verifier AP. The information includes the packet identification and type, the packet source, the packet destination, the packet's immediate sender (X), and the packet's immediate receiver (A). The verifiers expect that A will forward the

packet toward the ultimate destination, unless A is itself the destination. Each entry in the watch buffer is time stamped with a time threshold, s , by which A must forward the packet. Each packet forwarded by A with X as a previous hop is checked for the corresponding information in the watch buffer.

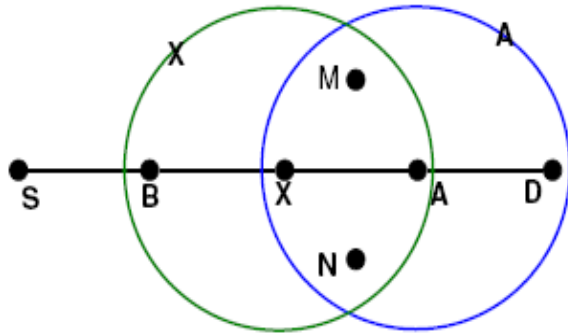


Figure 4. X, M, and N are Verifiers of A over the link from X to A.

V. DETECTION STRATEGY

- 1) Each AP has an RA (Responder of Access point) list of its Own and of its neighbors, If Any External AP pretends itself to be false Neighbor, it will be easily identified.
- 2) If Attack is on Internal AP, it can be checked in manner that- A malicious Log (Mal L(I,J)) is maintained at each Verifier AP, I, for a node, J, at the receiving end of each link that I is monitoring, For any malicious activity of J that is detected by I. The Log (Mal L) is created and forwarded to all the Neighbors of J and all link of J is dropped leading to prevention of desired attack.

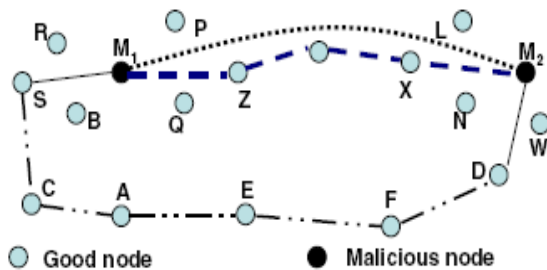


Figure 5. Malicious activity by M1 and M2

For example in Figure 5, the malicious Log (Mal L) of M1 and M2 are maintained by [P,Q,Z] and [L,X,N] over a link Z-M1 and X-M2 respectively. If M1 claims that it had receive packets from M2, the verifier AP of M1 will look in its watch buffer and detects the malicious activity of M1 and they will declare the M1 to Malicious AP and will send alert message to all neighbors of M1.

A. Algorithm

1. Broadcast a HELLO to all the neighbors
2. \forall responses

- Initialize RA
3. Broadcast RA to all neighbors and request for their RA's
4. \forall responses
Store RA of Neighbors
4. Initialize Watch buffer
5. Set (Mal L) =0
6. If (Communication Request (CR) arrives from Any Access Point (ID))
If (Check ID in RA)
Allow communication
goto step 7
Else
Discard communication
goto step 8
- /* Verification*/
7. If (accept packets from neighbor access point)
If ((Source and destination of coming packet) \in Stored RA of Neighbors)
Link verification
If (AP lies within vicinity of two or more Access Point)
Store in watch buffer \forall links
If (Mal L(I,J) \in Link from I to J)
Set (Mal L) =0
If (any malicious activity found)
Increment (Mal L) by 1
Broadcast Alert Message to all Neighbor
Go to step 5
8. End

B. Benefits

Our proposed mechanism requires no clock synchronization and location information. No special Hardware is required by this mechanism like GPS (Global Positioning system etc) for detection of wormhole. This mechanism will reduce the cost burden because it does not require extra devices. This mechanism also does not require any software tool for detecting rouge access point.

CONCLUSION AND FUTURE WORK

Wormhole attacks are a powerful attack that can be conducted without requiring any cryptographic breaks. An attacker who conducts a successful wormhole attack is in a position to disrupt routing, deny service to large segments of a network. In this paper, we have presented taxonomy for possible worm hole attack using a Infrastructure based wireless Architecture. We have presented a mechanism that incorporates a detection strategy. The fundamental mechanism used is Neighbor Discovery and Link Verification that monitors traffic in and out of its neighboring AP and uses a data structure of first and second-hop neighbors. Our mechanism reduces the threat of wormhole attacks and requires no clock synchronization and location information. In future we will try to overcome some more sophisticated wormholes using Mobile agents.

REFERENCES

- [1] Using Directional Antennas to Prevent Wormhole Attacks, Lingxuan Hu David Evans Department of Computer Science University of Virginia Charlottesville, VA [lingxuan, evans]@cs.virginia.edu
- [2] C. Karlof, D. Wagner, Secure routing in sensor networks: attacks and countermeasures, at the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.
- [3] Y.C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: Proceedings of the 22nd INFOCOM, 2003, pp. 1976–1986
- [4] L. Hu, D. Evans, Using directional antennas to prevent wormhole attacks, in: Proceedings of Network and Distributed System Security Symposium, 2004.
- [5] B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A secure routing protocol for ad-hoc networks,” Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.
- [6] 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.
- [7] Y. C. Hu, A. Perrig, and D.B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp. 1976-1986, 2003.
- [8] Defense Advanced Research Projects Agency. Frequently Asked Questions v4 for BAA 01-01, FCS Communications Technology. Washington, DC. Available at http://www.darpa.mil/ato/solicit/baa01_01faqv4.doc, October 2000.
- [9] S. Capkun, L. Buttya'n, J.-P. Hubaux, SECTOR: secure tracking of node encounters in multihop wireless networks, in: Proceedings of the First ACM Workshop on Security of Ad hoc and Sensor Networks (SASN 03), 2003, pp. 21–32.
- [10] L. Hu, D. Evans, Using directional antennas to prevent wormhole attacks, in: Proceedings of Network and Distributed System Security Symposium, 2004.
- [11] Y. Ko, V. Shankarkumar, N. Vaidya, Medium access control protocols using directional antennas in ad hoc networks, in: Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2000, pp. 13–21.
- [12] R. Choudhury, X. Yang, R. Ramanathan, N. Vaidya, Using directional antennas for medium access control in ad hoc networks, at the 8th ACM International Conference on Mobile Computing and Networking (MobiCOM), 2002.