An Effective Approach for the Detection of Wormhole Attack using Smart Antennas

Anitha S Sastry,
Asst Professor,
Dept of Electronics and Communication,
Global Academy of Technology, Bangalore-560098

***Abstract*— In this paper, a focus on securing communication over wireless data networks from wormhole attacks by using smart antennas is proposed. While conventional cryptography-based approaches focus on hiding the meaning of the information being communicated from the wormholes, here a complimentary class of strategies that limit knowledge of the existence of the information from the wormholes is considered. A profile the performance achievable with simple beamforming strategies using a newly defined metric called exposure region. Then the strategy within the context of an approach called Aegis, which uses virtual arrays of physical arrays to significantly improve the exposure region performance of a wireless LAN environment. This paper presents an analysis of wormhole attacks and proposes a countermeasure using smart antennas. It greatly diminishes the threat of wormhole attacks.**

I. INTRODUCTION

Securing communication in data networks has been a problem of interest since the time of conception of network-based communication. With the explosive growth in the usage of wireless data networks over the last several years, increasing attention is now being paid to specifically securing communication in wireless environments. Cryptography-based techniques including the Wired Equivalent Privacy (WEP), the WiFi Protected Access (WPA), and the IEEE 802.11i WPA2 all are examples of techniques that specifically protect wireless communication against some of these challenges. One of the primary properties of such cryptography-based techniques is that they hide the meaning of the information being communicated, but not the existence of the information itself. In other words, it is typically assumed that the adversary has access to all the information and the techniques are designed to make it computationally hard for the adversary to understand the true meaning of information. In this paper, we focus on a somewhat orthogonal form of securing communication that is sometimes referred to as physical space security. While the term encompasses a wide variety of techniques, it typically refers to approaches that limit knowledge of the existence of the information at the adversary. The scope of this paper is restricted to securing communication over wireless data networks and further limited to a specific form of adversarial behavior—eavesdropping and wormhole attack.

In particular, proposed routing protocols cannot prevent wormhole attacks. In a wormhole attack, an attacker introduces two transceivers into a wireless 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.

Next we provide background on secure routing protocols and previous work on preventing wormhole attacks. Section 3 considers wormhole attacks and analyzes their effectiveness. Section 4 introduces smart antennas and describes the strategy we use. Section 5 describes our protocols for verifying neighbor relationships.

II. SCOPE AND BACKGROUND

A. Scope

1)Environment: The wireless environment considered is that of a wireless local area network (WLAN) which consists of wireless APs, each equipped with an

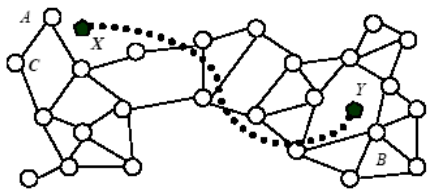

Figure 1:Wormhole attack

element antenna array and one or more clients, each equipped with a single omnidirectional antenna or an array of up to elements. Channel parameters such as line of sight (LOS), the degree of fading, and the richness of scattering vary widely for different indoor environments. Thus, to begin with, we consider a strong LOS path between an AP and each client.

Several secure routing protocols have been proposed for wireless ad hoc networks. Papadimitratos and Haas [13] present the SRP protocol that secures against non-colluding adversaries by disabling route caching and providing end-to-end authentication using an HMAC primitive. SEAD [2] uses one-way hash chains to provide authentication for DSDV [11]. Wormhole attacks depend on a node misrepresenting its location. Hence, location based routing protocols have the potential to prevent wormhole attacks [9]. Localization may be done using globally accessible beacons that broadcast known locations (that may be pre-configured or determined using

GPS [14]). Recently there has been some research to build localization system using localized protocols [15, 8, 5, 10]. The location service itself may become the attack target. Localization systems generally require some seed nodes that know their own positions, which may not be possible in all network environments.

B. Background

A previous approach for detecting wormhole attacks is to use packet leashes [4]. A temporal packet leash places a bound on the lifetime of a packet that restricts its travel distance. The sender includes the transmission time and location information in the message, and the receiver checks that the packet could have traveled the distance between the sender and itself within the time between reception and transmission.

C. Enhancing Security Using Smart Antennas

The approach to preventing wormhole attacks is for nodes to maintain accurate information about their neighbors (nodes within one hop communication distance). This is simpler than using location since each node need only maintain a set of its neighboring nodes. A message from a non-neighboring node is ignored by the recipient. Note that any protocol used to maintain accurate neighbor sets may itself be vulnerable to wormhole attacks, so our goal is to design a neighborhood discovery protocol that is not vulnerable to wormhole attacks. The security of our protocol will rely on using *virtual array of physical arrays*, where multiple access points (APs) in the same administrative domain, each equipped with a physical antenna array, are used in tandem to achieve the strategies and cooperation among nodes to verify possible neighbors.

III. WORMHOLE ATTACKS

In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network [4, 9]. Figure1 shows a basic 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*.

For most routing protocols, the attack has impact on nodes beyond the wormhole endpoints' neighborhoods also. Node *A* will advertise a one-hop path to *B* so that *C* will direct packets towards *B* through *A*. For example, in on-demand routing protocols (DSR [6] and AODV [16]) or secure on-demand routing protocols (SEAD [2], Ariadne [3], SRP [13]), the wormhole attack can be mounted by tunneling ROUTE REQUEST messages directly to nodes near the destination node. Since the ROUTE REQUEST message is tunneled through high quality channel, it arrives earlier than other requests. According to the protocol, other ROUTE REQUEST messages received for the same route discovery will be discarded. This attack thus prevents any other routes from being discovered, and the wormhole will have full control of the route. The attacker can discard all messages to create a denial-of-service attack, or more subtly, selectively discard certain messages to alter the function of the network. An attacker with a suitable wormhole can easily create a sinkhole that attracts (but does not forward) packets to many destinations. An intelligent attacker may be able to selectively forward messages to enable other attacks.

To show how much damage a single wormhole can cause to routing, we simulated randomly distributing nodes in a rectangular region and used the shortest path algorithm to find the best route between any node pairs. If a wormhole is formed, some far away nodes will appear to be neighbors and some node pairs will be able to find a "shorter" path through the wormhole. Hence the route between them is disrupted by the wormhole. In simulation experiments, a single wormhole with two randomly placed endpoints disrupts over 5% of all network routes.

A more intelligent attacker may be able to place wormhole endpoints at particular locations. Strategically placed wormhole endpoints can disrupt nearly all communications to or from a certain node and all other nodes in the network. If the base station is at the corner of the network, a wormhole with one endpoint near the base station and the other endpoint one hop away will be able to attract nearly all traffic from sensor nodes to the base station. If the base station is at the center of the network, a single wormhole will be able to attract traffic from a quadrant of the network. Figure 2 shows the effectiveness of a wormhole in disrupting communications from sensor nodes to a base station.

One endpoint of the wormhole is within one hop of the base station; the position of the second endpoint varies along the *x* axis. When the base station is in a corner of the network, a wormhole with the second endpoint near the base station can effectively disrupt all network communications. If the second endpoint is placed in the opposite corner, approximately half of the nodes in the network will send messages for the base station to the wormhole.

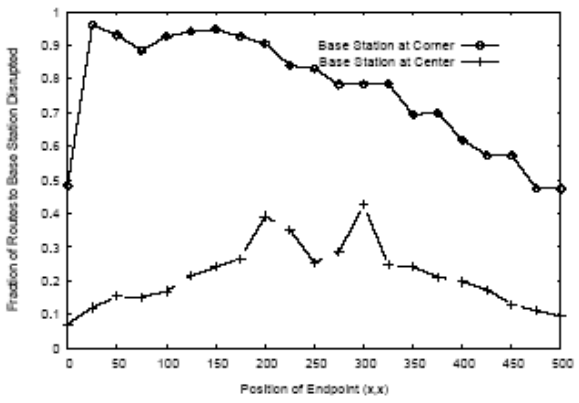

Figure 2: Impact of wormhole attack

IV. SMART ANTENNAS

Adaptive array smart antennas employ an array of antenna elements coupled with both amplitude and phase weighting, thereby making it possible to tune and obtain a large set of angular and spatial patterns. Thus, with adaptive arrays, it is possible to manipulate the weights on the different elements to obtain a desired pattern. At the simplest level, the process of forming a beam or main lobe to a certain direction is called beamforming. More formally, it is the process of choosing

antenna element weights such that the signal-to noise ratio (SNR) at the receiver is maximized. Also, when a strong LOS path is unavailable or multipath is rich, simple beam steering is less effective, and the pattern that maximizes the receiver's SNR does not necessarily have a main beam pointing toward the direction of the client [17]. This is particularly true in indoor environments, and the beams have to be adapted based on the channel condition. With appropriately chosen weights, adaptive arrays can be used to maximize the signal quality at the receiver even in the presence of channel impairments. Also, depending on whether the weight adjustments are performed at the transmitter or receiver, the technique is called transmit beamforming or receive beamforming, respectively [18]. Hence, the key properties of smart antennas that we leverage are as follows.

Property 1: A transmitter can control where it causes interference by the appropriate placement of nulls in its pattern.

Property 2: A receiver can null interference only from up to transmissions. Beyond that, it is unable to decode or resolve the transmissions.

Property 3: It is sufficient for either the interfering transmitter to suppress interference to an unintended receiver or for that receiver to suppress interference from an unintended transmitter.

Property 4: When more than parallel transmissions happen within an interference range, all transmissions suffer a reduction in signal-to-interference-plus-noise ratio (SINR) that will make the signal undecodable.

Wireless Security: While tapping the wired channel could require sophistication in device and physical manipulation of the medium, wiretapping can be done in a passive manner in the wireless channel. Consequently, even a casual user could turn into an false node. Furthermore, the actual security solutions are not as secure as the underlying cryptographic schemes due to practical difficulties such as improper key management. In addition to this, the wireless medium introduces new security issues such as user fingerprinting [19] and passive security attacks [20], which are not directly addressed by cryptographic schemes. These attacks motivate another dimension of security on top of existing security techniques.

V. ENHANCING SECURITY BY DETECTING WORMHOLE NODES

Our approach for detecting wormhole attacks depends on nodes maintaining accurate sets of their neighbors in the exposure region of beamforming between wireless nodes using smart antennas. When a transmitter, receiver, or both perform beamforming the signal is contained in a specific region between them depending on the beam patterns, the channel and the wormhole antenna capability. By sharing information among neighboring nodes, the verified neighbor discovery protocol along with information deprivation can prevent wormhole attacks where the attacker controls only two end points which are at least two hops distance.

A. *Assumptions*

We assume all non wormhole communication channels are bidirectional: if A can hear B , then B can hear A.

We assume a mechanism is available to establish secure link between all pairs of nodes and that are critical messages are encrypted. Many such mechanisms have been proposed for establishing secure link keys in wireless networks[1,7,12].

Using smart antennas beamforming technology, the neighbor nodes can be discovered and can prevent wormholes from rebroadcasting the message, and receiving any information from the neighboring nodes use of the following notation:

A,B,C,…….	Legitimate nodes
X,Y	Wormhole endpoints
R	Nonce
$E_{KAB}(M)$	Message encrypted by key shared between nodes A and B

B. *Verified neighbor discovery protocol with information deprivation*

The wormhole attack can be prevented if nodes cooperate with their neighbor. The nodes in other location can establish the announcer's legitimacy. We call such nodes as verifiers.

Immediately after deployment, nodes will have no known neighbors. Each node will randomly chose a time and periodically use verified neighbor discovery protocol to update its neighbor set. We call the node that initiates the protocol the announcer.

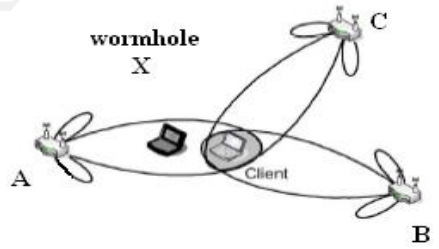

Figure 3: shows X is an wormhole sitting between legitimate nodes A and B where C is the verifier

We use verifier node to establish legitimate neighbor node relationships. This relies on all nodes having beamforming towards the client. The verified neighbor discovery protocol works as follows:

1. A→B HELLO||ID_A
2. B→A ID_B||E_{KBA}(ID_A|R| beamform(N,A))
3. A→B R

These steps authenticate the nodes and their apparent positions, but do not establish that they are communicating without going through wormhole. Next, the protocol uses verifier node to conform the link is not being created through a wormhole:

4. N→Region INQUIRY|ID_N|ID_A| beamform(N,A)

All neighbor nodes that hear the HELLO message broadcast an inquiry. If N received the announcement in one beamform, it will send inquiries to find the verifiers to the beamforms

which are attached to it. So, the prospective verifiers can determine if they satisfy the verification properties by having heard A in a different beamform.

5. C→N $ID_C|E_{KNC}(ID_A|beamform(C,N)$

Nodes that receive the inquiry and satisfy the verification properties respond with an encrypted message. This message confirms that the verifier heard the announcement in a different beamform from B.

To continue the protocol, B or N must receive at least one verifier response. If it does, it accepts A as a neighbor, and since message to A :

6. B→A $ID_B|E_{KAB}(ID_A|ACCEPT)$

After receiving the acceptance messages the announcer adds N to its neighbor sets.

The verified neighbor discovery protocols depends on both neighbor and verifier nodes receiving correct responses from the announcer before either node well accept announcer as a neighbor. This is vulnerable, however, to a wormhole attack in which a single endpoint node acts as both a receiver and a retransmitter to deceive that they are neighbors.

If there is a node in the beamform region attached to both the nodes A and B, then it can act as a verifier. However the verifier region may still exist when two nodes are slightly out of radio ranges

If node B is located just beyond the transmission range of node A, their will be two areas that could have valid verifier for this protocol. If this is the case, the attacker can just put one node in between A and B and use it to listen to and retransmit messages between A and B as shown in figure 4. Now the attacker can have control over all the messages transmitted between A and B.

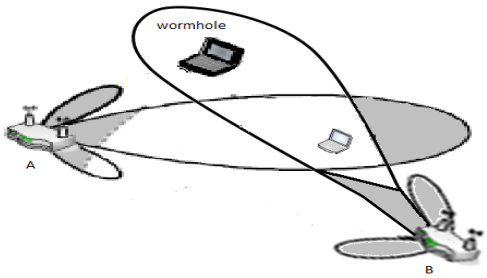

Figure 4: Represents false node placed between A and B and retransmitting messages between A and B

This attack will succeed only if the nodes A and B(in figure4) are unable to communicate directly, but are close enough to have it verifier that can hear both A and B. so assuming perfect transmission distances, this means A and B must be more than d a distance apart. The exposure area when using omni directional antenna can be given as-

$$\mathbf{A=\pi d^2}$$

The distance *d* can be measured from the transmission power and the free space propagation laws, given a receive power threshold P_{th} as follows :

$$d = \left(\frac{P_t * G_t * G_r * (\lambda)^2}{4 * \pi * P_{th}} \right)^{\frac{1}{\alpha}}$$

where P_t is the transmit power, G_t and G_r are main lobe gains of the transmit and receive antenna, α is the path loss exponent, and λ is the wavelength used. Let A' refer to the area with a sector model. It can be written as

$$A' = \frac{1}{2} d^2 * \theta$$

Where θ is the null–null beam width of the transmitting or receive antenna.

If A and B are aligned horizontally, the size of area it could contain false verifiers is

$$4 \int_{\frac{d}{2}}^{\frac{d\sqrt{3}}{2}} \left(\sqrt{1-x^2} - \frac{x}{\sqrt{3}} \right) dx$$

where d + a is the distance between A and B The maximum area is slightly less than 16% of the transmission area in the worst case where A and B are just d distance apart, and decreases substantially as distance increases. The verified neighbor discovery protocol prevents wormhole attacks when the adversary has only two end points. An attacker with multiple end points could selectively forward packets through to different end points to establish false neighbors. This can be prevented by information deprivation among two legitimate nodes.

Information deprivation

The underlying principle of information deprivation is to ensure that the false node is unable to receive information from separate transmissions occurring in the time, frequency, or spatial dimensions. Thus, the basic idea is to ensure that each piece of information is decodable only if multiple spatially separated transmissions can be decoded successfully. The idea with an instance of this approach called "*secret sharing*."

- ***Secret Sharing:***

Overview: The basic idea of secret sharing is well established in the context of cryptography [21]. In a general *t-out-of-n* secret sharing scheme, a secret message should be divided into n shares as $x \rightarrow (x_1,x_2,x_3..x_n)$ such that the following properties are satisfied.

• *Recoverability:* Given any *t* shares, *x* can be recovered.

• *Secrecy:* Given any t' <t shares, absolutely no information can be learned about *x*, i.e., the probability of learning *x* given *t' t* shares is the same as that of learning *x* with no shares, Pr(*x* |*t' shares*)=Pr(*x*).

Mechanism: The mechanism exploits the fact that when a single client is reachable from multiple APs, different shares of the message can be distributed to the clients through those APs. An worm hole in any position in the vicinity of the client

or APs would only be able to gain access to a fraction of the information due to the *spatially disjoint nature of the transmissions* that are possible with adaptive arrays unlike with omni antennas. The multiple elements of the array are utilized to perform beamforming, and the scheme is implemented in a time-division manner. Thus, the exposure region is the region of the network where all the shares (i.e., the packet fragments) of at least one data packet can be decoded successfully.

In this regard, we consider the *all or nothing encryption* (as proposed by Rivest [22]). which is a mechanism to prevent parts of a message from being recovered until the whole message is received in its entirety. This method involves encrypting the message with the key, and the key with the message blocks, thus rendering each unusable until the whole sequence (key and message) is correctly received.

VI. CONCLUSION

In this paper, the following conclusions are made

- Wormhole attacks are a powerful attack that can be conducted without requiring any cryptographic breaks. Smart antennas with the proposed idea offer a promising approach to prevent wormhole attacks.
- The protocols we propose reduce the threat of wormhole attacks with the minimal loss of network connectivity.
- This approach can be extended to eavesdrop attack also.
- Another proposed idea of detecting wormhole attack is to use virtual grid in order to detect neighbor nodes.

REFERENCES

[1] L. Eschenauer and V. Gligor. *A Key-Management Scheme for Distributed Sensor Networks*. ACM Conference on Computer and Communication Security, November 2002.

[2] Y. Hu, D. Johnson, and A. Perrig. *SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks.* IEEE Workshop on Mobile Computing Systems and Applications, June 2002.

[3] Y. Hu, A. Perrig and D. Johnson. *Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks*. ACM MobiCom 2002, September 2002.

[4] Y. Hu, A. Perrig, and D. Johnson. *Packet Leashes: A=Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. INFOCOM 2003, April 2003.

[5] T. He, C. Huang, B. Blum, J. Stankovic and T. Abdelzaher. *Range-Free Localization Schemes for Large Scale Sensor Networks.* ACM MobiCom 2003, September 2003.

[6] D. Johnson, D. Maltz, and J. Broch. *The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks.* In Ad Hoc Networking, C. Perkins, Ed. Addison-Wesley, 2001.

[7] H. Chan, A. Perrig and D. Song. *Random Key Predistribution Schemes for Sensor Networks.* IEEE Symposium on Security and Privacy 2003.

[8] N. Bulusu, J. Heidemann and D. Estrin. *GPS-less Low Cost Outdoor Localization for Very Small Devices.* IEEE Personal Communications Magazine, October 2000.

[9] C. Karlof and D. Wagner. *Secure Routing in Sensor Networks: Attacks and Countermeasures*. First IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.

[10] D. Niculescu and B. Nath. *Ad Hoc Positioning System (APS) using AoA.* INFOCOM 2003.

[11] C. E. Perkins and P. Bhagwat. *Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobilecomputers.* ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications,1994.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler and D. Tygar. *SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal*, September 2002.

[13] P. Papadimitratos and Z. Haas. *Secure routing for mobile ad hoc networks.* SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002

[14] B. Wellenhoff, H. Lichtenegger and J. Collins. *Global Positions System: Theory and Practice*, Fourth Edition. Springer Verlag, 1997

[15] R. Nagpal, H. Shrobe and J. Bachrach. *Organizing a Global Coordinate System from Local Information on an Ad Hoc Sensor Network*. 2nd International Workshop on Information Processing in Sensor Networks (IPSN '03), April, 2003.

[16] C. Perkins and E. Royer. *Ad-Hoc On-Demand Distance Vector Routing*. IEEE Workshop on Mobile Computing Systems and Applications, February 1999.

[17] M. Buettner, E. Anderson, G. Yee, D. Saha, A. Sheth, D. Sicker, and D. Grunwald, "A phased array antenna testbed for evaluating directionalityin wireless networks," in *Proc. MobiEval*, San Juan, Puerto Rico,Jun. 2007, pp. 7–12.

[18] A. Paulraj, R. Nabar, and D. Gore, *Introduction to Space-TimeWireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[19] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proc. ACM MobiCom*, Sep. 2007, pp. 99–110.

[20] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D. Sicker, "Passive data link layer 802.11 wireless device driver fingerprinting," in *Proc. USENIX Security Symp.*, Jul. 2006, Article no. 12.

[21] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[22] R. L. Rivest, "All-or-nothing encryption and the package transform," *Lecture Notes Comput. Sci.*, vol. 1267, p. 210, 1997.