Wormhole Attack in Wireless Ad-Hoc Networks

Yahya Ghanbarzadeh, Ahmad Heidari, and Jaber Karimpour

***Abstract*—Wormhole attack is a severe attack in wireless ad-hoc networks. To establish a wormhole attack, attackers create a direct link, referred to as a wormhole tunnel, between them. Wormhole tunnels can be occurring by means of a wired link, a high quality wireless out-of-band link or a logical link via packet encapsulation. After building a wormhole tunnel, one attacker receives and copies packets from its neighbors, and forwards them to the other colluding attacker through the wormhole tunnel. However they need special hardware to support such communication.**

In this paper, we propose an efficient method to detect, secure and avoid wormhole attacks. We have introduce a special packet with name WADP packet that when a node suspect to a wormhole attack, sends it for his cluster head and to own cluster head too. Each node that receive WADP packet updates his routing table by dropping wormhole route from his table. Finally all nodes on the network receives WADP packet and drops malicious nodes information's from his routing tables.

***Index Terms*—Ad-hoc networks, cluster, malicious nodes, wormhole attack.**

I. Introduction

Wireless ad hoc networks are networks that are create for specific purposes and nodes in this networks can be connect each other without having fixed infrastructure like access points. Routing between any of two nodes in these networks is difficult because each node can move randomly entire the network and sometime even leave the network. This means one path that is an optimal now, may be after a few seconds this path doesn't exist at all. So routing protocols in wireless ad hoc networks must be dynamic. Since the wireless ad hoc networks are growing these days, the important note in using this technology knows strengths and weaknesses of them. Security, like most another network issues, can be on demand or not. All of these criteria in the case of network protocols security related on routing algorithms operation. Attacks on the wireless ad hoc networks can by win these defined criteria, and disrupt the network performance. Attacks on ad hoc network routing protocols generally fall into one of two categories [1]:

1) Routing-disruption attacks: The attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. An example of a routing-disruption attack is for an attacker to send forged routing packets to create a routing loop, causing packets to traverse nodes in a cycle without reaching their destinations, thus consuming energy and available bandwidth. A more subtle type of routing-disruption attack is creating a wormhole in the network, using a pair of attacker nodes A and B linked via a private network connection.
2) Resource-consumption attacks: The attacker injects packets into the network in an attempt to consume valuable Network resources such as bandwidth or to consume from an application-layer perspective; both attacks are instances of a denial-of-service (DoS) attack.

A wormhole attack [2][3][4] is composed of two attackers and a wormhole tunnel. To establish a wormhole attack, attackers create a direct link, referred to as a wormhole tunnel, between them. Wormhole tunnels can be established by means of a wired link, a high quality wireless out-of-band link or a logical link via packet encapsulation. After building a wormhole tunnel, one attacker receives and copies packets from its neighbors, and forwards them to the other colluding attacker through the wormhole tunnel. This latter node receives these tunneled packets and replays them into the network in its vicinity. In a wormhole, attackers are directly linked to each other, so they can communicate swiftly. However they need special hardware to support such communication. On the other hand, a wormhole using packet encapsulation is relatively much slower, but it can be launched easily since it does not need any special hardware or special routing protocols. Furthermore, the attackers can mount the attack without revealing their identities [5]. Most routing protocols like AODV and DSR are vulnerable against this attack. In wormhole attack, attackers want to violations Availability، Integrity and Reliability of the network.

Fig. 1 shows a basic wormhole attack [4]. 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.

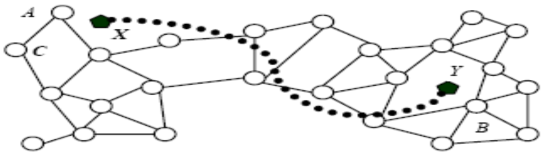

Fig. 1. Wormhole attack. The adversary controls nodes X and Y and connects them through a low-latency link.

For most routing protocols, the attack has impact on nodes beyond the wormhole endpoints' neighborhoods also. Node

Manuscript received February 19, 2012; revised March 30, 2012.

Y. G. is with the Department of Computer Engineering, Islamic Azad University, Ajabshir Branch, Ajabshir, Iran (e-mail: Yahya_bonab@yahoo.com).

A. H. is with the Department of Computer Engineering, Islamic Azad University, Ajabshir Branch, Ajabshir, Iran (e-mail: a.heidari@ajabshiriau.ac.ir).

J. K. is with the Department of Computer Science, Tabriz University, Tabriz, Iran (e-mail: jaber_karimpour@yahoo.com).

A will advertise a one-hop path to B so that C will direct packets towards B through A. 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 [4].

This paper is divided into total of five sections. Section 1 consists of introduction. In section 2 we review related works about problem. Section 3 consists our approach for detecting wormhole attack. Section 4 gives analyses and evaluation our method And Section 5 concludes with the conclusion.

II. Background

Several approaches have been developed to defend against wormhole attacks in mobile ad hoc networks. The existing methods against the wormhole attack can be divided into proactive and reactive countermeasures [7].

Proactive methods attempt to prevent wormhole formation, typically through specialized hardware used to achieve accurate time synchronization or time measurement, or to transmit maximum power in a particular direction. Among proactive methods, timing-based solutions attempt to restrict the maximum distance between two neighbors by computing the packet travel time. In [2], the authors introduce packet leashes as a countermeasure against the wormhole attack. There are two types of packet leashes: geographic leash and temporal leash. In geographic leash, for example, when node “A” sends a packet to node “B”, must add its location information and sending time into the packet. And node “B” can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes clocks is bounded by Δ, and this value should be known to all the nodes. By using metrics mentioned above, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is discarded.

Unlike Packet Leash, Capkun et al. [3] presented SECTOR which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD) Node. An estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash is. A similar approach is used in [8] for secure single-hop pair wise time synchronization. In practice, all of the aforementioned timing-based methods suffer from some of the following shortcomings [7].

1) The nodes require synchronized clocks;
2) Each node has to be capable of fast switching between the receive and send modes;
3) Each node needs one-to-one communication with all its neighbors;
4) Each node requires predicting the sending time and computing signature while having to timestamp the message with its transmission time.

In [7], nevertheless that is timing-based countermeasure does not have any of these shortcomings, and thus is more suitable for practical implementation of solutions based on packet travel time measurements but this method is also proactive method and uses specialized hardware to achieve accurate time synchronization or time measurement, or to transmit maximum power in a particular direction.

In [4], directional antennas are used to prevent against wormhole attacks. Each node in the network shares a secret key with every other node and broadcasts HELLO messages to discover its neighbors using directional antennas in each direction.

Qian et.al [9] Design a statistical analysis on the frequency of each link among multi-path. The detection is based on the observation that the link which spans the wormhole will occur more often in routing paths. However, this cannot be used to detect hidden wormhole attack because multiple links can be affected by one wormhole. Each link could occur in different paths. The affected link can be just like a normal link from its frequency value. Then the statistical analysis fails.

In [10], the proposed DelPHI protocol allows a sender to observe the delays associated with the different paths to a receiver. Therefore, a sender can check whether there are any malicious nodes sitting along its paths to a receiver and trying to launch wormhole attacks. The obtained delays and hop count information of some disjoint paths are used to decide whether a certain path, among these disjoint paths, is under a wormhole attack.

Reactive methods, on the other hand, don’t need specialized hardware and time synchronization or time measurement, or to transmit maximum power in a particular direction [7]. For example, the proposed source routing protocols in [12] and [13] consider the wormhole as a valid link and avoid it only if it exhibits some malicious behavior like modifying or dropping packets but this methods cannot prevent wormhole attacks. This is achieved using some basic mechanisms such as packet authentication and destination acknowledgment. In this paper, we proposed a better reactive method to detect and avoid wormhole attack in ad hoc networks.

III. Proposed Method

Before we describe the mechanism, we first represent some definitions and then briefly describe our system requirements and assumptions.

We define a cluster head node while a node wants connect more than two nodes. In fig. 2 we displayed them with blue color. Each cluster head are connected with other cluster heads with one or more hops, and in each cluster head’s routing table, moreover the distance until his cluster members, distances between neighbors cluster head’s written. Malicious nodes are nodes that make virtual tunnel between each other that we call wormhole. In fig. 2 we displayed them with red color. WADP1 packet (consist wormhole route

[1] Wormhole Attack Detection Packet

information): When a node suspect one route to be in wormhole tunnel, sends a WADP packet to his nearest cluster head and his routing table members nodes.

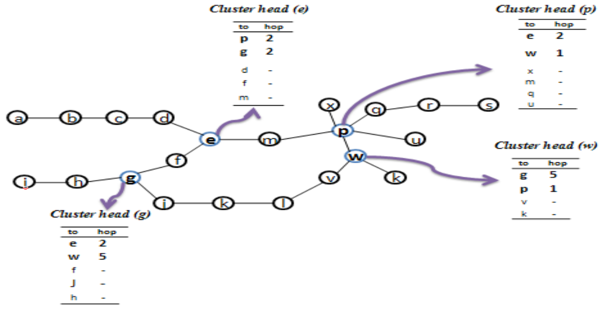

Fig. 2. Clustering network nodes and defining cluster heads routing tables.

The transmission power of a wormhole is similar to a normal node in that more powerful transceiver is easily to be detected. We assume that the malicious nodes can control the communication between two nodes S and D if and only if the shortest paths between them include a virtual tunnel. We assume that all nodes in our network use asymmetric key cryptography for securing. We also assume that moreover than a tunnel that maybe be between two nodes, another route also have between that nodes.

A. Cluster Formation

In this paper, we analyze the effect of the wormhole attack on shortest-path routing protocols. We have proposed an algorithm where intrusion detection has been done in a cluster based manner to take care of the wormhole attacks. We divide the entire network geographically into a few clusters. And clusters are monitored by cluster heads. Using the proposed solution, the nodes do not need to have synchronized clocks, and are not required to predict the sending time or to be capable of fast switching between the receive and send modes. Moreover, the nodes do not need to communicate with all their neighbors one-to-one and communicate with cluster heads. As you see in fig. 2 the entire network is divided in clusters and each cluster has its own cluster head and a number of nodes designated as member nodes. Member nodes pass on the information only to the cluster head. The cluster head is responsible for passing on the aggregate information to all its members. The cluster head is elected dynamically and maintains the neighboring node information plus neighboring cluster head nodes information's in its own routing table. Another nodes in the network, only stores its neighboring node information in its routing table and nodes that most entries of routing tables are similar to their will be in same clusters. Also every node has a unique id in the network, which is assigned to a new node collaboratively by existing nodes.

B. Cluster Based Detection Technique

In some routing protocols of wireless ad hoc networks, for example, AODV [14] and DSR [11], the source node first initiates a routing discovery by broadcasting a ROUTE REQUEST packet. All intermediate nodes continues broadcasting the ROUTE REQUEST upon receiving it until the ROUTE REQUEST reaches the destination or some nodes that have a route to the destination. Then a ROUTE REPLY will be unicasted back to the source along a pre-cached path (e.g. in AODV, all intermediate nodes cache a reverse path to the source during the broadcasting) or according to the path in the packet header (e.g. the packet header of DSR has the entire route).

Next, we present the algorithm to detect wormhole attacks. We describe our method in three modes:

1) The wormhole attack can severely affect routing protocols based on shortest delay and shortest path by delivering packets faster and with a smaller number of hops, respectively [2]. When a node wants to send a packet, at first all routes until destination will be found with broadcasting ROUTE REQUEST and ROUTE REPLY packets. After that, a private key will send to destination, from a route that is bigger than the shortest route then we initialize to send packets. We also add one flag bit with name R/W[2] to all packets that we send. This R/W flag bit has this characteristic that when a node wants modify packet, the data of this bit will be clear. Therefore recipient will be announcing of eavesdropping. And will send a WADP packet to his cluster head node and that cluster head will broadcast that packet to all neighbor cluster heads. And in parallel cluster heads send that packet for his cluster members. Each node that receive WADP packet updates his routing table by dropping wormhole route from his table. Finally that route information will dropped from all nodes routing tables. Therefore with this technique, attackers cannot read or write any of packets.

2) We send all packets between nodes (that are in different clusters) from the cluster heads to each other, unless a tunnel is between two nodes. We consider that all tunnels are secure and we send all packets from shortest paths with shortest path routing protocols. In sending packet from the source to the destination, maybe one or all of packets drops during tunnel. This dropping packet is because of two reasons: a) maybe the physical or wireless link between nodes are disconnected. In this case if sender, don't receive ack packet from receiver after a specified time slice, will send WADP packet for his cluster head node. b) Malicious nodes drop all packets or some of them and make them on irregular sequence. In this case if the receiver, revives packets on irregular sequence, will send a WADP packet to his cluster head.

   In that two manners a and b, after cluster head receives WADP packet, will broadcast that packet to all neighbor cluster heads. And in parallel cluster heads send that packet for his cluster members. Each node that receive WADP packet updates his routing table by dropping wormhole route from his table. Finally that route information will dropped from all nodes routing tables. Therefore with this technique, if attacker drops some or all packet, or if the route disconnect, another nodes on the network will detect that, and will avoid sending packet from that route.

3) Sometimes malicious nodes records one packet at one end point and relayed to the other end and re-broadcasted into the network. Furthermore, the attackers can mount the attack without revealing their

[2] Read/Write Flag Bit

identities [2]. This kind of attack is because of that the senders IP is valid and known's for all nodes on the network and they don't suspect him. Attackers can make traffic and lose bandwidth with sending one packet more and more in the network. For detecting this kind of attack, receiver can periodically check header file that one packet don't send more than one time for receiver. And for avoiding that, receiver will send WADP packet to his cluster head to announce other nodes, that route is unsecure and must remove from all routing table.

Now we explain this method with an example. At real communications between neighbors are radio transmission and the radio link between neighbors is bidirectional but in this example because of simplicity we consider wired links between nodes. In fig. 3, suppose two nodes "m1" and "m2" are malicious nodes and virtually using wired links or a high quality wireless out-of-band links and are neighbors with each other (suppose at first other nodes don't know that these nodes are malicious, therefore these route don't known's as a wormhole tunnel). In this figure suppose node "a" wants to sends a packet (or packets) for node "s". If the routing protocols are on demand, at first node "a" broadcasts ROUTE REQUEST packet for his neighbors and after middle nodes broadcast this packet until it receives to node "s" in three routes with names α, β and γ that α is: (a→b→c→d→e→m→p→q→r→s) and β is: (a→b→c→d→e→f→g→j→k→l→v→w→p→q→r→s) and γ is: (a→m1→m2→s) and ROUTE REPLY packet will unicast on backward to the sender. As you see cost of route α is 9 hop, cost of route β is 15 hop and cost of route γ is 3 hop therefore route γ is the shortest path and data's from "a" to "s" will send from this route. Now, node "a" will send a private key to node "s" from route α and data packets from γ. if malicious nodes wants to read/write the packets constant, the R/W flag bit value will clear and "s" after receiving packet and observe the R/W value, while this bit value cleared, will send WADP packet to "p" and "p" also will broadcast that packet for nodes that are in his routing table (e.g. e,w,x,q,u,m) and every nodes that receives that packet will broadcast it for his routing table members and Finally all nodes on our network that received WADP packet, will remove γ route information from his routing tables.

If malicious nodes wants to drop some packets of sending packets, and make irregular sequence packets or when drops all packets and don't receive packets to "s". "s" will send a WADP packet to "p" and every nodes that are in his routing table. This act will be continuing until every node receives that packet and drupes wormhole route from his table. Therefore with this method, attackers cannot drop packets. maybe malicious nodes wants to records one packet at one end point like "m1" or "m2" and sends that more and more in the network for making traffic. In this mode; receiver, periodically will check header file that one packet don't send more than one time for him. And for avoiding that, if receiver receives one packet more than one time, will send WADP packet to his cluster head and every nodes that are in his routing table, to announce other nodes, that route is unsecure and must remove from all routing table

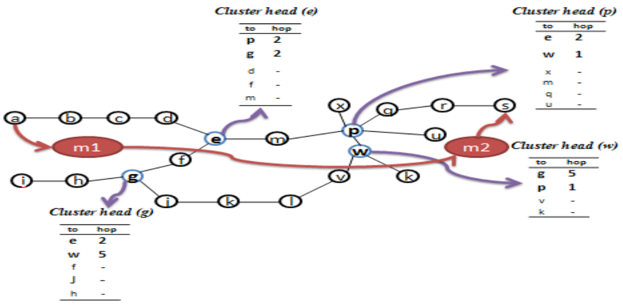

Fig. 3. An example of wormhole attack.

IV. Analysis and Evaluation Results

Here we analyze our method in more detail, this method can use secure in unsecure networks that use shortest path to send packets. At first, before sending data packets to destination, from all routes until destination will be found with broadcasting ROUTE REQUEST and ROUTE REPLY packets. Then, a private key will send to destination, from a route that is bigger than the shortest route then we initialize to send packets. Then even the shortest path be unsecure, cannot change or drop packets and we can use the shortest path for reducing cost.

Now suppose route γ in fig. 3 is unsecure and mayme be a wormhole tunnel. Therefore if route γ don't change or drop our packets, we will use this route else we drop this route and send packet from route α. if the cost of sending packet between two 1-hop neighbors be 1x and if we consider fig. 3 example, that node "a" wants to send N packets to node "s", cost of sending packets by our method can be reachable as bellow:

$$all\ cost\ of\ sending = W_{\alpha}x + N\,(W_{\gamma}x) \qquad (1)$$

That's because of a private key packet will send from route α and all data packet (N) will send from route γ. But if we don't use that tunnel and send all packets from route α, cost of sending will be as bellow:

$$all\ cost\ of\ sending = N\,(W_{\alpha}x) \qquad (2)$$

For example in fig. 3, suppose node "a" wants sends 100 packets to destination "s". If all packets use (2) for sending, cost of sending will be about 900x and if all packets sends from route β, the cost of our sending will be about 1500x. But in our method, that use (1) for sending, therefore cost of sending will be about 309x. with this risk that we do, if route γ not be wormhole tunnel and be a secure route we only lose a few cost (about 9x cost because of sending private key from route α).

Next for evaluate our method; we compare that with other four main wormhole detection methods: packet leash [2], SECTOR [3], directional antennas method [4] and EDWA [5]. The results are shown in Table 1, where the requirements for each method is listed in column two to column four and the detection method is compared in column five. For the defending method, packet leash and SECTOR aim to prevent.

Wormhole by restricting the transmission distance of each hop either using life time in the packet header or distance bounding. Directional antenna maintains correct neighborhood using a verifier. All above methods can only detect wormhole or avoid the affection of wormhole attack. EDWA can effectively identify wormhole using wormhole TRACING. But our method can effectively detect and avoid wormhole by using R/W bit and WADP packet.

TABLE I: COMPARING REQUIREMENTS AND USAGE OF FOUR MAIN METHODS WITH OUR METHOD

Method	Geographical Device	Clock Synchronization	Other Special Requirements	usage
Packet leashes [2]	Yes	Strong	No	Detect and Avoid
SECTOR [3]	No	Loose	Module For Single Bit Communication	Detect and Avoid
Directional Antenna [4]	No	No	Directional Antennas (special hardware)	Detect and Avoid
EDWA [5]	Yes	No	No	Detect and Identify
Our Method	No	No	R/W Flag Bit and WADP Packet	Detect, Secure and Avoid

V. CONCLUSION AND FUTURE WORKS

In this paper, we have introduced the wormhole attack, as a sever attack that can have serious consequences on many proposed ad hoc network routing protocols. Our proposed method can detect unsecure routes that can be created by malicious nodes. If attackers want to read/write the constant of packet, an R/W flag bit value will clear and receiver will suspect accruing wormhole attack and detect that. And if malicious nodes wants to drop some packets of sending packets, and make irregular sequence packets or when drops all packets and don't receive packets to destination at all and or when physical or wireless link between nodes are disconnect, our method can detect the attack or removed links better. We can avoid against wormhole attack on ad hoc networks too. For avoiding wormhole attack in this networks, we propose special packet with name WADP packet that when a node suspect to one route, will send a WADP packet to his cluster head node and that cluster head will broadcast that packet to all neighbor cluster heads. And in parallel, cluster heads send that packet for his cluster members. Each node that receive WADP packet updates his routing table by dropping wormhole route from his table. Finally that route information will dropped from all nodes routing tables and avoid from wormhole attack. We also by sending a private key to destination from a route that is bigger than the shortest route then initialize to send packets can use even the unsecure shortest paths and reduce cost of sending packets.

We would like to research work explore another idea in wormhole attack detection and simulate our proposed method with ns-2 simulator [15]. Our studies will improve a new approach for detecting this kind of attacks.

REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", *Published By The IEEE Computer Society, IEEE*, 2004 .

[2] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole Attacks in Wireless Networks," in *Proc. INFOCOM*, 2003.

[3] S. Capkun, L. Buttyan, and J. P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *Proc. First ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[4] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. Network and Distributed System Security Symposium*, 2004.

[5] X. Wang and J. Wong, "EDWA: End-to-end detection of wormhole attack in wirelesss ad-hoc networks." *International Journal of Information and Computer Security (IJICS)*, under revision, July 2007.

[6] L. Lazos1, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks" *Washington*, 2004.

[7] Majid Khabbazian, Hugues Mercier, and Vijay K. Bhargava, "Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, February 2009.

[8] K. Sun, P. Ning, C. Wang, A. Liu, and Y. Zhou, "TinySeRSync: secure and resilient time synchronization in wireless sensor networks," in *Proc. 13th ACM Conference on Computer and Communications Security*, 2006.

[9] L. Qian, N. Song, and X. Li. "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path." *Wireless Communications and Networking Conference*, Mar. 2005. vol. 4, pp. 2106 – 2111.

[10] 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, Jan. 2006.

[11] D. B. Johnson, D. A. Maltz, and Y. Hu. "The dynamic source routing protocol for mobile ad hoc networks (DSR)." *IETF MANET Internet Draft*, 2003.

[12] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on demand secure routing protocol resilient to byzantine failures," in *ACM Workshop on Wireless Security (WiSe)*, 2002.

[13] I. Avramopoulos, H. Kobayashi, R. Wang, and A. Krishnamurthy, "Highly secure and efficient routing," in *Proc. INFOCOM*, 2004.

[14] C. E. Perkins, E. M. Royer, and S. R. Das. "Ad-hoc ondemand Distance vector routing." In *the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90–100, Feb. 1999.

[15] "The Network Simulator ns-2," At: http://www.isi.edu/nsnam/ns.