Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure

Majid Khabbazian, Hugues Mercier and Vijay K. Bhargava
Department of Electrical and Computer Engineering
University of British Columbia
2356 Main Mall, Vancouver, BC, Canada V6T 1Z4

***Abstract*— The wormhole attack is one of the most severe security attacks in wireless ad hoc networks. In this paper, we analyze the effect of the wormhole attack in shortest path routing protocols. Using analytical and simulation results, we show that a strategic placement of the wormhole can disrupt on average 32% of all communications across the network. We also analyze a more severe attack in which several attackers make wormholes between each other and give an upper bound on the average number of communications that can be disrupted. Finally, we propose a new robust and secure on-demand distance vector routing protocol which is able to route packets as long as there is a non-faulty path between the source and the destination.**

I. Introduction

The *wormhole attack* [1] is one of the most severe security attacks which can significantly disrupt the communications across the network. Moreover, it is hard to detect and easy to implement. In a wormhole attack, the attacker receives packets at one location in the network, "tunnels" them to another location and replays them there. A single malicious node can launch this attack by for example broadcasting the route requests at a high power level. The wormhole attack is even more powerful if it is launched by more than one attacker. In this case, attackers can tunnel the packets to each other by simply encapsulating them or by using an out-of-band link. Once a wormhole is established, malicious nodes can use it to make a Denial-of-Service (DoS) attack by for instance dropping certain data or control packets.

The wormhole attack can be launched in two different modes. In the *hidden mode*, the attackers do not use their identities so they remain hidden from the legitimate nodes. In fact, the attackers act as two simple transceivers which capture messages at one end of the wormhole and replicate them at the other end. In this way, they can make a *virtual link* between two far-off nodes by for example "tunneling" the HELLO messages. The existing wormhole detection schemes [1], [2], [3] typically consider this mode. Clearly, the attackers require no cryptographic keys to launch the wormhole attack in the hidden mode.

In the *participation mode*, the attackers can launch a more powerful attack by using valid cryptographic keys. In this mode, the attackers make no virtual links between the legitimate nodes. In fact, they participate in the routing as legitimate nodes and use the wormhole to deliver the packets sooner or with smaller number of hops. As in the hidden mode, the attackers can drop data packets after being included in the route between the source and the destination.

In this paper, we analyze the effect of the wormhole attack in shortest path routing protocols. Using our new model, we show that a strategic placement of the wormhole can disrupt on average 32% of the communications across the network. We also show that $(n \geq 2)$ attackers can disrupt on average at most $(1-\frac{1}{n})$ of all the communications. The results are further confirmed by simulation. We then propose a new routing protocol to counter a variety of attacks including the wormhole attack. It is, to the best of our knowledge, the first on-demand distance vector protocol that can avoid the wormhole attack in participation mode. Using the proposed countermeasure, the source and the destination are able to communicate as long as there is at least one non-faulty path between them.

The rest of the paper is organized as follows. In Section II, we present and categorize related work on the subject. In Section III, we introduce a new analytic model to measure the effect of the wormhole attack and present simulation results corroborating our model. We propose a robust and secure distance vector routing protocol in Section IV and conclude the paper in Section V.

II. Related Work

The existing countermeasures against the wormhole attack can be divided into proactive and reactive countermeasures. Proactive countermeasures attempt to prevent wormhole formation, typically through specialized hardware. For example, in [1], the authors introduce packet leashes as a countermeasure against the wormhole attack. In their method, the source node adds some information such as its precise location or time to the packet in order to restrict the packet's maximum transmission distance. A similar approach is used in [2], where each node can estimate the distance to another node by sending a challenge bit and receiving its instant respond. In [4], a small fraction of network nodes called guards have access to location information (for example using GPS) and are assigned specific network operations. Directional antennas can also be used to mitigate the wormhole attack [3]. All of the above methods require specialized hardware to achieve accurate time synchronization or time measuring, or to transmit maximum power in a particular direction. Furthermore, the main drawback of these methods is that they cannot detect a wormhole running in the participation mode. It is due to the fact that they attempt to

prevent wormholes between two legitimate nodes; however, in the participation mode, the wormhole is formed between two malicious nodes participating in the routing. Note that in this mode, all the links are valid except the one (the wormhole) between the two attackers.

Reactive countermeasures, on the other hand, do not prevent the wormhole formation. For example, the proposed source routing protocols in [5] and [6] consider the wormhole as a valid link and avoid it only if it exhibits a Byzantine behavior. This is achieved by using some basic mechanisms such as packet authentication and destination acknowledgment. In this paper, we use a similar approach to propose a robust and secure on-demand distance vector routing protocol. The proposed protocol allows only authenticated nodes to participate in the routing. It also assume that the authenticated nodes may exhibit Byzantine behaviors. This assumption makes our protocol more robust compared to the existing secure on demand distance vector routing protocols such as ARAN [7].

III. Wormhole Attack Analysis

The wormhole attack can severely affect the routing protocols based on shortest delay and shortest path by delivering packets faster and with smaller number of hops, respectively. The common belief is that the wormhole attack can prevent nodes from discovering other nodes that are more than two hops away [1], [8]. In this section, we analyze the effect of the wormhole attack in shortest path routing protocols and show that on average any node is able to discover and communicate with at least 50% of all other nodes across the network. We assume that our network consists of a large number of nodes distributed uniformly with density δ inside a disk of radius R. We also assume that any two nodes are able to directly communicate with each other if the distance between them is less than or equal to T.

In shortest path routing protocols, hop count is typically used as a metric to select the path with the minimum number of hops. In order to find the actual shortest path, each intermediate node has to increase the hop count by one. We assume that a hop count hash chain [9] is used to protect the hop count from being decreased, thus a malicious node can at most refuse to increase the hop count to attract data packets.

Let us define $d_{S,D}$ as the distance between nodes S and D, and $N_{S,D}$ as the number of hops of the shortest path between them. Clearly, we have

$$N_{S,D} \geq \frac{d_{S,D}}{T}. \tag{1}$$

Lemma 1: In a network with limited diameter and high node density, with high probability we have

$$N_{S,D} \leq 2\frac{d_{S,D}}{T}.$$

Proof: The number of nodes in a region $\mathcal{R}$ with area $\Delta_{\mathcal{R}}$ follows a Poisson distribution [10], since they are uniformly and independently distributed. It follows that

$$\text{P}(\mathcal{R} \text{ contains } k \text{ nodes}) = e^{-\delta\Delta_{\mathcal{R}}}\frac{(\delta\Delta_{\mathcal{R}})^k}{k!}. \tag{2}$$

If $d_{S,D} \geq \frac{T}{2}$, then there are $t = \lfloor 2\frac{d_{S,D}}{T}\rfloor - 1$ disks with radius $\frac{T}{4}$ and origins at distances $d_i = \frac{T}{2}i + \frac{T}{4}$, $1 \leq i \leq t$, from S on the line going through S and D. This is illustrated in Figure 1. Using (2), we get

$$\begin{aligned}\text{P(at least one node in each disk)} &= (1 - \text{P(no node in a disk)})^t \\ &= (1 - e^{-\delta(\pi(\frac{T}{4})^2)})^t.\end{aligned}$$

Clearly, the distance between two nodes in adjacent disks is at most T. Therefore, there is a path of length $t+1 = \lfloor 2\frac{d_{S,D}}{T}\rfloor$ with probability at least $(1 - e^{-\delta(\pi(\frac{T}{4})^2)})^t$. Consequently, we have $N_{S,D} \leq \lfloor 2\frac{d_{S,D}}{T}\rfloor \leq 2\frac{d_{S,D}}{T}$ with high probability when

$$e^{-\delta(\pi(\frac{T}{4})^2))}t \ll 1 \quad \text{or} \quad \delta \gg \frac{\ln(\lfloor 2\frac{d_{S,D}}{T}\rfloor - 1)}{\pi(\frac{T}{4})^2},$$

where $d_{S,D} \leq 2R$. Note that the assumption of uniform distribution is not a necessary condition. In other words, the same result can be obtained if $P_0 \ll \frac{T}{2R}$, where P_0 is the probability of having no node in a disk with radius $\frac{T}{4}$ and with the origin inside the network. ■

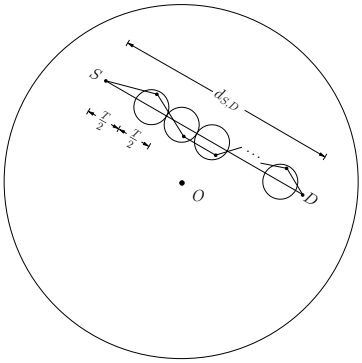

Fig. 1. Finding a path between S and D.

From (1) and Lemma 1, we observe that $N_{S,D}$ is a function of $\frac{d_{S,D}}{T}$ and can be approximated by

$$N_{S,D} = \beta\frac{d_{S,D}}{T}, \tag{3}$$

where $1 \leq \beta \leq 2$.

Lemma 2: The malicious nodes M_1 and M_2 can disrupt the communication between the nodes S and D if

$$\min(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}) \leq d_{S,D}.$$

Proof: Recall that the malicious nodes can refuse to increase the hop count. Therefore, the path through M_1 and M_2 (or M_2 and M_1) looks shorter than the actual shortest path between S and D if and only if

$$\min(N_{S,M_1} + N_{D,M_2} - 1, N_{S,M_2} + N_{D,M_1} - 1) < N_{S,D}.$$

Using (3) we get

$$\min(\beta\frac{d_{S,M_1}}{T} + \beta\frac{d_{D,M_2}}{T}, \beta\frac{d_{S,M_2}}{T} + \beta\frac{d_{D,M_1}}{T}) \leq \beta\frac{d_{S,D}}{T},$$

thus

$$\min(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}) \leq d_{S,D}.$$

When the malicious nodes are on the path, they can disrupt the communication by dropping the route reply or data packets. ■

Let us assume that the malicious nodes M_1 and M_2 are located at the coordinates $(-m, 0)$ and $(m, 0)$, respectively. As shown in Figure 2 , the perpendicular bisector l of the line segment M_1M_2 partitions the network into two regions $\mathcal{R}_1$ and $\mathcal{R}_2$ containing M_1 and M_2, respectively.

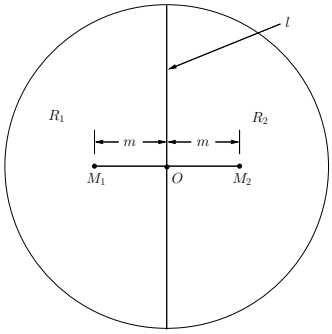

Fig. 2. Partitioning the network into regions $\mathcal{R}_1$ and $\mathcal{R}_2$.

Lemma 3: Let S and D be two nodes both inside $\mathcal{R}_1$ or $\mathcal{R}_2$. We have

$$\min\left(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}\right) > d_{S,D}.$$

Proof: Without loss of generality, we can assume that both S and D are in $\mathcal{R}_1$. Hence,

$$(d_{S,M_2} > d_{S,M_1}) \text{ and } (d_{D,M_2} > d_{D,M_1}).$$

Therefore, using the triangle inequality, we obtain

$$\min\left(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}\right) > d_{S,M_1} + d_{D,M_1} \geq d_{S,D}.$$

■

From Lemmas 2 and 3 it follows that two nodes in the same region are able to communicate. Let P_1 and P_2 be the probability that a randomly selected node is in region $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively. Clearly, $P_1 + P_2 = 1$ and the probability that two randomly selected nodes are in the same region is

$$P_1^2 + P_2^2 = 0.5 + \frac{(P_1 - P_2)^2}{2} \geq 0.5.$$

Therefore, the attackers cannot disrupt on average more than 50% of all communications across the network.

Definition 1: A region is called unreachable for a node S if it is inside the network and if for any node D in the region

$$\min\left(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}\right) \leq d_{S,D}.$$

We denote the largest unreachable region for a node S as U_s. From Lemma 2, it follows that the wormhole attack can disrupt the communications between a node S and any node in U_s. The following proposition gives more precise information regarding the severity of a wormhole attack initiated by two malicious nodes M_1 and M_2.

Proposition 1: Let S be a randomly selected node in $\mathcal{R}_1$ and Δ_{U_s} be the area of U_s. We have

$$\Delta_{U_s} = \frac{1}{2}\int_{\theta_{-1}}^{\theta_1} (g^2(\theta) - f^2(\theta))d\theta,$$

where

$$f(\theta) = \frac{d_{S,M_2}^2 - d_{S,M_1}^2}{2(d_{S,M_2}\cos(\theta) - d_{S,M1})},$$

$$g(\theta) = d_{S,M_1}\cos(\theta + \gamma) + \sqrt{R^2 - d_{S,M_1}^2 \sin(\theta + \gamma)},$$

$\gamma = \angle OSM_2$, O is the origin of the network and the values θ_1 and θ_{-1} are the roots of the equations $(g(\theta) - f(\theta) = 0)$ and $(g(-\theta) - f(\theta) = 0)$, respectively.

Proof: Let D be a node in U_s. According to Definition 1,

$$\min\left(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}\right) \leq d_{S,D}. \quad (4)$$

Since the node S is in $\mathcal{R}_1$, it follows from Lemma 3 that the node D is not in $\mathcal{R}_1$. Therefore,

$$\min\left(d_{S,M_1} + d_{D,M_2}, d_{S,M_2} + d_{D,M_1}\right) = d_{S,M_1} + d_{D,M_2}. \quad (5)$$

From (4) and (5) it follows that

$$d_{S,M_1} \leq d_{S,D} - d_{D,M_2}.$$

The equation $d_{S,M_1} = d_{S,D} - d_{D,M_2}$ defines a branch of the hyperbola with foci S and M_2. Therefore, as shown in Figure 3, U_S is a region between the network boundary (a circle of radius R) and the branch of the hyperbola. Let us consider S as the origin and SM_2 as the x-axis of a polar coordinate system. Using the cosine rule for the triangles SM_2E and SOF, we can compute $f(\theta)$ and $g(\theta)$, respectively. The area Δ_{U_s} can then be computed with

$$\Delta_{U_s} = \int_{\theta_{-1}}^{\theta_1}\int_{f(\theta)}^{g(\theta)} r dr d\theta.$$

■

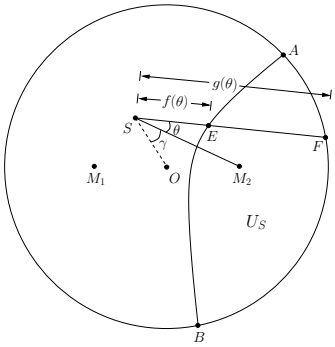

Fig. 3. Computing the area of U_s using polar coordinates.

Consider a polar coordinate system with origin O (the origin of the network) and x-axis OM_2. Let (r, α) be the polar

coordinates of a node S. The expected value of Δ_{U_s} can be calculated from

$$E[\Delta_{U_s}] = \frac{4}{\pi R^2} \int_{\alpha=\frac{\pi}{2}}^{\pi} \int_{r=0}^{R} \Delta_{U_{(r,\alpha)}} r dr d\alpha. \qquad (6)$$

As finding a closed form for (6) is difficult (if not impossible), we compute it numerically. Figure 4 shows the numerically computed $E[\Delta_{U_s}]/(\pi R^2)$. As shown in the figure, $E[\Delta_{U_s}]/(\pi R^2)$ is maximized when the attackers M_1 and M_2 are located at the coordinates $(-0.33R, 0)$ and $(0.33R, 0)$. For the simulation, the radius of the network is set to $R = 1$ and 500 nodes are randomly put inside the network. We run the simulation for the transmission ranges $T = 0.2$ and $T = 0.15$. In the simulation, a communication is considered affected by the attack if the shortest path through the wormhole is shorter than the legitimate shortest path between the source and the destination. The simulation is then repeated a few hundred times in order to obtain the average percentage of affected communications across the network. As shown in Figure 4, both the simulation and the analytical results indicate that two malicious nodes can disrupt 32% of all communications across the network when they initiate a wormhole attack.

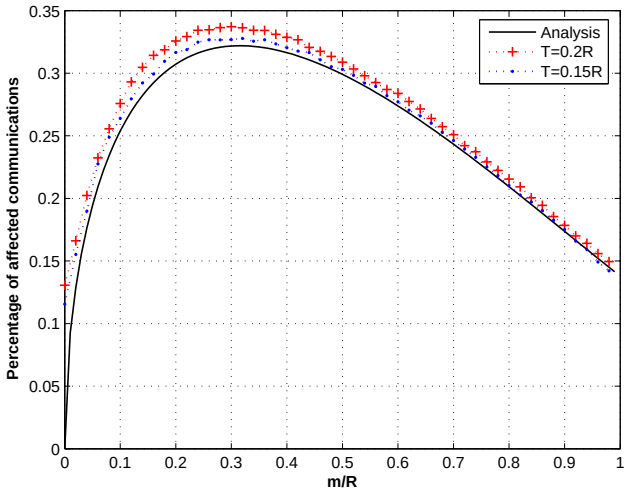

Fig. 4. Percentage of affected communications across the network.

Now, consider the case where $(n \geq 2)$ malicious nodes attack the network by making wormholes between each other. In this case, a malicious node can send packets to any other malicious node using a path of wormholes. Clearly, this generalized wormhole attack can disrupt more communications across the network. The following proposition gives an upper bound on the average percentage of affected communications.

Proposition 2: Let $M_1, M_2, \ldots, M_n$ be $(n \geq 2)$ malicious nodes making wormholes between each other. On average, at least $\frac{1}{n}$ of all communications across the network are not affected by the attack.

Proof: As shown in Figure 5, the network can be partitioned into n regions or Voronoi cells [11] such that each cell contains exactly one malicious node and every point is closer to the malicious node in its cell than the others. Let S and D be two nodes inside a cell with the malicious node M_g. Using the Voronoi cell definition and the triangle inequality, we have

$$d_{S,D} \leq d_{S,M_g} + d_{D,M_g} < d_{S,M_i} + d_{D,M_j},$$

where $1 \leq i, j \leq n$ and $i \neq j$. Thus, the malicious nodes cannot disrupt the communication of two nodes inside the same cell. Suppose P_i is the probability that a node is in the cell C_i. Therefore, we have $\sum_{i=1}^{n} P_i = 1$. The probability that two randomly selected nodes are in the same cell is $\sum_{i=1}^{n} P_i^2$. From the Cauchy-Schwartz inequality, it follows that

$$\sum_{i=1}^{n} P_i^2 \geq \frac{(\sum_{i=1}^{n} P_i)^2}{n} = \frac{1}{n},$$

hence the probability that the communication between two randomly selected nodes S and D is not affected by the attack is at least $\frac{1}{n}$. ■

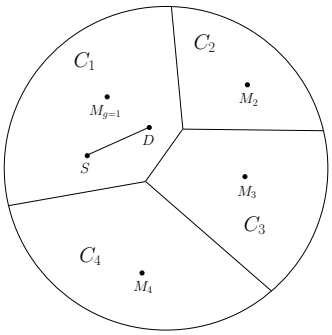

Fig. 5. Partitioning a network with several attackers into Voronoi Cells.

IV. Wormhole Attack Countermeasure

In this section, we present a secure and robust distance vector routing protocol. In the proposed protocol, we can use either the delay or the hop count as a metric to make routing decisions. When the hop count is used, we employ a hop count hash chain [9] to protect it from being decreased. We assume that each legitimate node has a public-key certificate issued by a trusted Certificate Authority (CA), whose public key is known by all the nodes. To make the protocol robust against malicious behavior, we assume that the nodes with valid cryptographic keys can also attack the network.

A. Route Discovery

In the route discovery phase, the source and/or the destination nodes typically use flooding in order to discover a path between each other. In our proposed protocol, we assume that some techniques such as digital signature verification and buffer reservation are used to protect the nodes from being congested by a flooding attack. We also assume that the network links are bidirectional as it is required by many wireless Medium Access Control protocols such as *IEEE* 802.11.

In the first step of the route discovery phase, the source node S generates a *Route Request* (RREQ) packet, signs it using its private key and broadcasts it to its neighbors:

$$S \rightarrow \text{brdcast: } [PI, RI, IP_D, N_S]\text{Sig}_S, \text{Cert}_S.$$

The RREQ packet consists of a packet identifier (PI) which includes some information such as packet type (e.g., RREQ). The RREQ packet also includes a request identifier (RI), the destination IP address (IP_D), a nonce (N_S), the source signature (Sig_S) and the source certificate (Cert_S) (note that the source IP address (IP_S) is included in the certificate). Both N_S and RI are incremented monotonically, but N_S is increased for each routing packet while RI may remain the same for several route discovery attempts. When an intermediate node receives an unprocessed RREQ packet, it first compares the nonce N_S to the last nonce received from S, validates the source signature and then rebroadcasts the verified packet. This step should be carried out as quickly as possible since its only goal is to inform the destination that the source node intends to communicate with it. Consequently, this step requires no hop count or extra authentication.

When the destination node D receives the first legitimate RREQ from S, it initiates the second step by broadcasting a *Route Reply* (RREP) packet:

$$D \rightarrow \text{brdcast: } [PI, RI, IP_S, N_D]\text{Sig}_D, \text{Cert}_D.$$

Note that a broadcast is required in order to guarantee that the RREP packet reaches the source node. The RREP packet requires a hop count and a hop count hash chain if the shortest path is desired. As in the first step, the first intermediate node A rebroadcasts a received RREP packet if the packet is verified. Before rebroadcasting the packet, A sets up a reverse path to D, adds a number H_{IP_A} to the RREP packet and signs the packet:

$$A \rightarrow \text{brdcast: } [[PI, RI, IP_S, N_D]\text{Sig}_D, H_{IP_A}]\text{Sig}_A, \\ \text{Cert}_D, \text{Cert}_A.$$

The next intermediate node B validates the packet, sets up a reverse path to D, removes A's certificate and signature, adds its number H_{IP_B} and then signs it:

$$B \rightarrow \text{brdcast: } [[PI, RI, IP_S, N_D]\text{Sig}_D, H_{IP_A}, H_{IP_B}]\text{Sig}_B, \\ \text{Cert}_D, \text{Cert}_B.$$

The subsequent intermediate nodes along the path behave like B. As in the ARAN protocol [7], intermediate nodes' signatures are used to ensure that only nodes with valid cryptographic keys can participate in the routing. The number H_{IP_X} is obtained by taking the first byte of $\text{Hash}(IP_X)$, where $\text{Hash}(.)$ is a hash function. As it will be explained later, these short numbers are added to the RREP packet by intermediate nodes to prevent a new attack which we call the *multipath attack*. Clearly, the numbers are not protected by the destination node's signature and can be modified by the intermediate nodes.

Upon receiving the RREP packet, the source node S initiates the last step by unicasting a *Route Establishment* (REST) packet to D:

$$S \rightarrow \text{unicast:}[PI, RI, IP_S, IP_D, N_S, (H_{IP_A}, H_{IP_B}, \ldots)]\text{Sig}_S.$$

It is worth mentioning that the REST, Acknowledgments (ACK) and data packets do not include any certificate as we assume that the intermediate nodes temporarily store the source and the destination public keys in the early steps of the route discovery phase. When an intermediate node E receives a REST packet from its neighbor F, it validates N_S, the sequence of hash numbers $(H_{IP_A}, H_{IP_B}, \ldots)$, F's signature and the source signature. The packet is dropped by E if the sequence of hash numbers does not start with $(H_{IP_A}, H_{IP_B}, \ldots, H_{IP_E}, H_{IP_F})$. If the packet is verified, the node E sets up a reverse path to the source S, removes F's signature, signs the REST packet and forwards it to the next node in the path to the destination. Note that the sequence of hash numbers is typically a few bytes and is only used in the second and third steps of the route discovery phase.

B. Packet Forwarding And Fault Avoidance

As in [5], [6], we use destination acknowledgment in order to guarantee the reception of the REST and data packets. Let F and E be two consecutive intermediate nodes along the discovered path from the source S to the destination D. If F receives a REST or a data packet from the source, it forwards it to E and sets a timeout, τ_F, equal to the worst-case Round-Trip Time (RTT) to the destination. The worst-case RTT can be approximated as $\tau_F = \kappa(T_r - T_b)$, where T_b is the time when F broadcasts the RREQ packet, T_r is the time when it receives the first corresponding RREP packet and $(\kappa \geq 1)$ is a constant known by all the nodes.

The node F unicasts a *Route Error* (RERR) packet to S if its link to E becomes broken. Moreover, When the timeout fires, it unicasts a Fault Report (FR) if it has not received any valid source acknowledgment, route error or fault report packet. Both RERR and FR packets have the form

$$F \rightarrow \text{unicast: } [PI, RI, IP_S, [\text{RREP}_E], N_F]\text{Sig}_F, \text{Cert}_F$$

and can be differentiated by their PI. The generated RERR/FR packet consists of the signed route reply packet RREP_E received by F from E at the second step of the route discovery phase. After unicasting the RERR/FR packet, the intermediate node F discards all the RREP packets from E with the request identification RI and the source IP address IP_S. Using this technique, the source node S can avoid the faulty links by using the same RI for the next route discovery phase. Note that by increasing the RI, the source node S can reuse the removed links which were previously reported faulty.

C. The Adversary

As mentioned earlier, our proposed protocol does not prevent the formation of a wormhole inside the network. However, it considers the wormhole as a single link which will be avoided if it exhibits Byzantine behaviors. For example,

consider the case where there is a wormhole between two intermediate nodes F and E. If the link between F and E is due to a wormhole attack launched in the hidden mode, then the link is treated as a valid single path. However, if the link exhibits a malicious behavior (such as dropping the packets), the node F will generate a fault report and will refuse to use the link in the next route discovery phase. Now, consider the case where two malicious nodes M_1 and M_2 launch the wormhole attack in the participation mode. Let us assume that F, M_1, M_2 and E are consecutive nodes along the path between the source and the destination. The malicious nodes cannot simply drop or modify the packets, unless they provide the node F with a signed destination acknowledgment or a signed RERR/FR packet. This is because the link between F and the malicious node M_1 will be considered faulty and will be avoided in the next route discovery attempts. Note that an attacker can only report the link to its neighbor as faulty because, in the RERR/FR packet, it has to include a valid route reply with a sequence of hash numbers identical to what the attacker used in the second step of the route discovery. Therefore, whether the malicious node generates a RERR/FR packet or not, a faulty link[1] will be detected and avoided.

The malicious nodes can launch a new attack called *multipath attack*. In the multipath attack, the malicious node M_2 forwards the same data packet to more than one of its neighbors. These neighbor nodes will then try to deliver the data packet to the destination. Consequently, a node along the path will receive at least two identical data packets and will drop the second one as a duplicate, thereby causing its upstream neighbor to generate a FR packet. The malicious node M_2 can then unicast the FR packet and drop the legitimate destination acknowledgment. Fortunately, the multipath attack can be countered using the sequence of hash numbers. Recall that the REST packet of the route discovery phase includes a sequence of hash numbers which is validated by each intermediate node. Hence, a malicious node cannot forward the REST and the data packets to more than one of its neighbors as the packet will be accepted by at most one of them.

D. Comparison with ARAN

The proposed protocol offers several security enhancements over ARAN. In ARAN, a malicious node can simply make a DoS attack by dropping the RREP packets. In this case, the source node may consider the destination as unreachable or unavailable. In our protocol, we address this problem by flooding the RREP packets. We also address data packet dropping problem by utilizing a timeout mechanism used in some secure source routing protocols such as [6]. The proposed protocol employs a sequence of hash numbers to counter the multipath attack. These numbers are not protected by the destination node's signature so they can be modified by malicious nodes. However, any modification of hash numbers will be reflected in the REST packet which would be detected and discarded by the attacker's downstream node.

[1]A link is faulty if it is broken or incident to a malicious/faulty node.

Finally, it is worth mentioning that the proposed protocol incurs more overhead than ARAN mainly due to the RREP flooding by the destination. This overhead can be reduced under certain circumstances (for example when the network is under "normal operation") by requiring the destination to unicast the RREP packet and use flooding only when it does not receive a REST packet. Note that in this case, intermediate nodes require to sign the RREQ packets in a similar way used for broadcasting the RREP packets.

V. Conclusion and Future Work

In this paper, we studied the effect of the wormhole attack in shortest path routing protocols. Using analytical and simulation results, we showed that two strategically located attackers can on average disrupt 32% of all communications across the network. We also considered the effect of the wormhole attack launched by $n \geq 2$ malicious nodes and showed that on average at least $\frac{1}{n}$ of all communications are not affected by the attack. Finally, we proposed a robust and secure on demand distance vector routing protocol to counter the wormhole attack launched in the hidden or participation mode. The proposed protocol uses digital signatures, destination acknowledgments and fault reports in order to remove the faulty links. It also employs a sequence of hash numbers in its route discovery phase to prevent the multipath attack.

The proposed protocol uses similar cryptographic primitives as ARAN, thus it can employ most of its optimization techniques. It would be desirable to further optimize the proposed protocol and to compare its performance with ARAN for the cases where the network is under an attack or works under normal operation. It would also be interesting to investigate the effects of the wormhole attack in shortest delay routing protocols.

References

[1] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," *In Proc. of INFOCOM*, 2003.

[2] S. Capkun, L. Buttyan, and J. P. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," *In Proc. of the first ACM workshop on Security of ad hoc and sensor networks*, 2003.

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

[4] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," *In Proc. of WCNC*, 2005.

[5] 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.

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

[7] B. Dahill, B. N. Levine, E. Royer, and C. Shields,, "A secure routing protocol for ad hoc networks," *In Proc.of the* 10^{th} *Conference on Network Protocols (ICNP)*, 2002.

[8] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop," *In Proc.of the International Conference on Dependable Systems and Networks*, 2005.

[9] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," *ACM WiSe*, 2002.

[10] A. Papoulis, *Probability and Statistics*. Prentice Hall, 1990.

[11] F. Aurenhammer and R. Klein. Voronoi diagrams. In J.-R. Sack and J. Urrutia, editors, *Handbook of Computational Geometry*. Elsevier Science Publishers, 2000.