2010 Fifth IEEE International Conference on Networking, Architecture, and Storage

A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information

Yun Wang Zhongke Zhang
School of Computer Science & Engineering
CNII, Southeast University
Nanjing, China, 210096

Jie Wu
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 119122

Abstract

Ad hoc networks are promising but are vulnerable to selfish and malicious attacks. One kind of malicious attack, hidden wormhole attacks, can be mounted easily and be immune to cryptographic techniques. Wormholes distort network topology, and degrade the performance of applications such as localization and data collection. A wormhole attack is one of the most severe threats to an ad hoc network. Unfortunately, most state-of-the-art wormhole detection algorithms are not practicable. We observe and prove that, nodes attacked by the same wormhole are either 1-hop neighbors or 2-hop neighbors, and with a high probability, there are 3 nodes, which are non-1-hop neighbors, in the intersection of the two neighbor. However, such phenomena will not be present in normal topology. Thus a novel distributed algorithm is designed for wormhole detection and isolation with polynomial complexity. The detection probability is discussed. Simulation results show that the algorithm performs well regarding detection probability, as well as network overhead, false node alarms and miss detection.

1 Introduction

Ad hoc networks are easy to be deployed in environments lacking communication infrastructures such as those for earthquake rescue, fire rescue, battlefields, etc. They are always multi-hop networks without central administration. Every node plays the role of both terminal and router. Distribution and autonomy are the key features of ad hoc networks. Most present protocols and mechanisms for ad hoc networks pay more attention to autonomy, without consideration of security. Ad hoc networks, however, are actually fragile. On the one hand, security approaches used in wired networks aren't suitable for autonomous networks, and on the other hand, ad hoc networks are exposed to more attacks because of their autonomy and distributed nature.

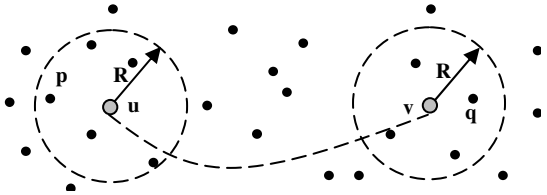


Figure 1: An example of wormhole attacks

Ad hoc networks are vulnerable to two kinds of menaces [6], i.e., selfish attacks and malicious attacks. Selfish nodes only benefit from others' services. Malicious nodes often fabricate, eavesdrop, and interrupt network communication or distort network topology to disrupt the operation of protocols. A wormhole [7] is one kind of severe malicious attack. It launches attacks by creating a "tunnel" between two remote nodes. Packets from one point are captured and then injected into another point. A wormhole distorts network topology, dramatically degrades the performance of such applications as localization and data collection, etc.

Wormholes can be categorized into two types: exposed and hidden wormholes [8]. The wormhole nodes in exposed wormholes behave as clean nodes. As depicted in Fig.1, nodes u and v are nodes in an ad hoc network. Both of them are compromised and serve as wormhole nodes. Nodes p and q are in $u's$ and $v's$ communication range, respectively. Both nodes are not in each other's communication range. Because of u and v, p regards the route to q as p-u-v-q. So does q. They falsely think they are quite near each other. In hidden wormhole attacks, u and v do not expose themselves to others. In the same scenario in Fig.1, p considers v as its 1-hop neighbor. Hidden wormhole attacks need not compromise any node, and other nodes do not feel the threat. By replaying packets form one end to another end, u and v need not analyze or temper the packets. Thus wormhole

978-0-7695-4134-1/10 $26.00 © 2010 IEEE
DOI 10.1109/NAS.2010.22

attacks are immune to cryptographic techniques. If ranging is accurate enough, q can check whether it has too many 1-hop neighbors with the same distance in order to detect a wormhole. Unfortunately, distance estimation errors by most current ranging techniques are so great that they are not feasible for real applications.

There is much literature that addresses the ad hoc security issues [1–6], and many have also achieved several good results. Some algorithms detect wormholes, based on geographical information and time or hop bound [7]. Some studies argue that any defense mechanism against a wormhole attack can be interpreted by a graph theoretic framework [8]. Some researchers look for forbidden structures from the network [10] to detect wormholes, while others detect wormholes through reconstructing network topology [11] or statistical analysis [12, 13].

We are interested in hidden wormhole attack detection in this paper. We observe that all the nodes affected by wormholes are either 1-hop neighbors or 2-hop neighbors under the UDG (Unit Disk Graph) model. The UDG [14] model states that any node $u's$ communication range is in the shape of a circle with $u's$ communication radius. Furthermore, we prove that in normal ad hoc networks, 3 nodes do not occur, which are mutually non-1-hop neighbors, in the intersection of the neighbor sets of u and v where v and u are 2-hop neighbors. If such a 3-node set regarding (u, v) exists, then u and v are affected by a wormhole. Therefore, the problem of detecting wormhole attacks turns out to be a problem of identifying whether a 3-node set exists in the intersection of the neighbor sets of specific nodes. A novel distributed algorithm with polynomial complexity is designed for wormhole detection and isolation. Detection probability is also analyzed. The simulation results show that the performance of the algorithm is satisfactory.

In summary, the contributions of the paper are as follows:

1. We prove that nodes attacked by the same wormhole are either 1-hop neighbors or 2-hop neighbors. Further if two nodes are affected by the same wormhole and are 2-hop neighbors, with a high probability, there are 3 nodes, which are non-1-hop neighbors, in the intersection of the two neighbor.

2. A novel elaborate distributed algorithm is designed for wormhole detection and isolation with polynomial complexity. The algorithm does not rely on specific hardware and it is easy to implement.

3. The theoretical detection probability of the algorithm is computed. The performance on detection probability, network overhead, miss detection and false node alarms ratios are evaluated by simulation. Results show that the algorithm performs well.

The remainder of the paper is organized as follows. In section II, we briefly introduce related work. The system model and terms are given in section III. We prove the theorems related to the neighborhood in section IV. In Section V, a novel elaborate algorithm for wormhole detection and isolation is presented. The theoretical analysis and experimental performance are described in section VI. Section VII concludes this paper.

2 Related Work

There is much literature that addresses the issue of defending against wormholes. In this section, we give a brief overview of these methods' principles and their pros and cons.

Methods based on positioning information. Hu et al [7] proposed to add geographical and temporal packet leashes to restrict transmission distances of packets. The method depends on positioning information and loosely synchronized clocks in geographical leashes or tightly synchronized clocks in temporal leashes. In [8], Poovendran et al introduced a method with special nodes called guards to provide protection. Initially, every guard generated a random fractional key FK_i and broadcasted it. The broadcast message also contained the coordinates (X_i, Y_i) of the guard. Any two nodes established a pairwise key from the common fractional keys they held. During this procedure, if any node received multiple copies of an identical message from the same guard or noticed that two guards were too far away, it assumed the network was under attack. This method also relied on positioning information and assumed that guards have higher transmission power.

Methods based on hop count and statistical analysis. Wang et al [9] proposed a model to estimate hop count with distances. A sender estimated the shortest path length from a source to a destination in terms of hop counts based on the two nodes' positions. If a path hop value was less than estimated, the path was under a wormhole attack with a high probability. The method's accuracy is doubted especially when confronting long distance paths. In [11], Wang et al presented a method with two steps. It first reconstructed the layout of a network using multi-dimensional scaling and then graphically visualized the occurrence of wormholes. It was a centralized algorithm. Khalil et al [12] proposed two algorithms called LiteWorp and MobiWorp for static and mobile ad hoc networks, respectively. Each node first discovered its neighbors within 2 hops and then detected potential wormholes based on local monitoring. They needed a certified authority to verify the truth of any location. Song et al [13] argued that a link affected by a wormhole may occur more often in routing paths. They detected wormholes by statistical analysis based on the frequency of each link among multi-paths. The method is only adapted to multi-

path routing protocols such as SMR.

Methods based on forbidden structures. Maheshwari et al [10] detected wormholes by looking for forbidden structures from a network. If there were too many independent common k-hop neighbors of any two nodes, a wormhole was detected. But it neglects the neighborhood information among nodes attacked by the same wormhole and lacks theoretic detection probability analysis.

Different from the above-named work, we further prove that if nodes u and v are attacked by wormholes, u and v are 1-hop neighbors or 2-hop neighbors. Further if u and v are affected by the same wormhole and are 2-hop neighbors, with a high probability, there are 3 nodes, which are non-1-hop neighbors, in the intersection of the neighbor sets of u and v.we also proposing a way to calculate the theoretic detection probability under UDG model.

3 System Model

3.1 Assumptions

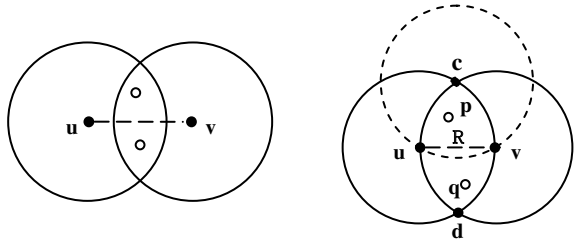
The UDG model is applied to each node in a network. Each node has the same communication radius R and the replaying radii of wormhole nodes are the same as R. We have a further discussion about the replaying radii in the Appendix. The links are bidirectional. We assume that nodes are randomly and uniformly deployed. The random deployment of the network nodes is modeled as a Spatial Homogeneous Poisson Point Process [15]. We further assume that wormhole will not replay messages. This assumption is reasonable, because if messages from node p are replayed to nodes within circle centered in node u, as depicted in Fig.1, p will received its own messages and part of p's neighbors will receive these messages more than once. They can easily find that they are attacked by wormholes.

We also assume that private/public keys have been deployed in the network. Every node in the network is able to sign its wormhole notification message packets with its private key, and each legal node can verify its signature with the public key.

3.2 Terms

$N_1(u)$ represents $u's$ 1-hop neighbors. It is a set of nodes which can communicate with u directly. $N_2(u)$ denotes $u's$ 2-hop neighbors. It is a set of nodes which are 1-hop neighbors of $u's$ 1-hop neighbors, but they are not $u's$ 1-hop neighbors. Hence, neighbors of u within 2 hops include $u's$ 1-hop neighbors plus $u's$ 2-hop neighbors represented by $N_1(u) + N_2(u)$.

The intersection of $N_1(u)$ and $N_1(v)$ is denoted as $C_1(u, v)$. $Suspects(u)$ is a set of nodes suspected to be attacked by a wormhole from the viewpoint of u.



(a) $d_{uv} \in (R, 2R]$ (b) $d_{uv} = R$

Figure 2: Node neighborhood in a normal network

Under the UDG model, the circle centered at u is denoted as CIR_u and the nodes in CIR_u as ND_u.

3.3 Problem statement

The wormhole detection problem lies in identifying the nodes which are attacked by wormholes. A wormhole node always sends the packets it receives to a remote wormhole node. If a network is attacked by wormholes, wormhole isolation is pursued in order to isolate and remove attacked nodes from a network. That is, they will not forward packets generated by these attacked nodes. Thus, a wormhole will not be able to disrupt the operation of network communication.

We recognize that the wormholes cause changes in a network topology and further observe that the neighborhood information is abnormal for those nodes affected by wormholes. We prove that the abnormal phenomenon does not occur in normal ad hoc networks. With this observation, we achieve the goal of figuring out a solution to the wormhole detection problem.

4 Theorems

Theorem 1. *Regarding any a pair of nodes (u,v) in a normal ad hoc network, there are at most 2 distinct nodes of* $C_1(u, v)$ *which are non-1-hop neighbors, i.e.,* $\mid S \mid \leq 2$ *if* $S \subseteq C_1(u, v)$ *and* $\forall p, q \in S \rightarrow p \notin N_1(q) \wedge q \notin N_1(p)$.

Proof. Without loss of generality, there are two nodes u and v. In a normal network, if u and v are 2-hop neighbors, the distance d_{uv} between u and v should satisfy $R < d_{uv} \leq 2R$ where R is $u's$ communication radius. The nodes of $C_1(u, v)$ appear in $CIR_u \cap CIR_v$, the overlappimg area as depicted in Fig.2(a). When d_{uv} is approaching R, the overlapped region turns out to be the largest, as shown in Fig.2(b).

In Fig.2(b), the area $\overline{uvc}$ surrounded by arc uv, vc and cu forms a equilateral arc-triangle. Therefore, the distance between any two nodes in $\overline{uvc}$ is not larger than R [16].

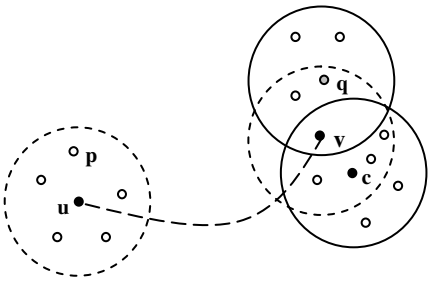


Figure 3: Node Neighborhood when a wormhole exists

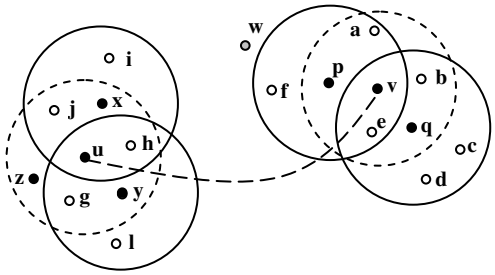


Figure 4: An Scenario that a wormhole distorts network topology

That is, any two nodes within $\overline{uvc}$ are 1-hop neighbors. For the same reason, any two nodes within $\overline{uvd}$ surrounded by arc uv, vd and du are 1-hop neighbors.

For any node $p \in \overline{uvc}$, $p's$ non-1-hop neighbors within area $\overline{ucvd}$ have to appear in $\overline{uvd}$. For the same reason, for any node $q \in \overline{uvd}$, $q's$ non-1-hop neighbors within the area $\overline{ucvd}$ have to appear in $\overline{uvc}$. There are three cases.

(i) No node in both $\overline{uvc}$ and $\overline{uvd}$. So $\mid S \mid = 0$ because $\mid C_1(u,v) \mid = 0$.

(ii) No node in $\overline{uvc}$ or $\overline{uvd}$. $\mid S \mid = 1$. All the nodes in $C_1(u,v)$ are 1-hop neighbors.

(iii) Both $\overline{uvc}$ and $\overline{uvd}$ are non-empty. Let S=$\{p,q\}$. Suppose that there is a node x in $\overline{ucvd}$, $x \neq p$ and $x \neq q$, and x is a 1-hop neighbor of neither p nor q. $x \notin N_1(p) \wedge x \notin N_1(q)$ holds. We have $x \notin \overline{uvc} \wedge x \notin \overline{uvd} \Rightarrow x \notin \overline{ucvd}$. It is contradictory to the hypothesis. So $\mid S \mid = 2$.

In all, $\mid S \mid \leq 2$.

□

Theorem 2. *Any two nodes within the communication range of the same wormhole are either 1-hop neighbors or 2-hop neighbors.*

Proof. Without loss of generality, u and v are the wormhole nodes in a wormhole. As shown in Fig.3, ND_u and ND_v are attacked by a wormhole directly. It is obvious that there are two nodes, for example, p and q, are 1-hop neighbors.

Now we discuss the part about 2-hop neighbors. In a normal network, owing to the fact that there is no node in the intersection of the neighbor sets of q and c, q is not a 2-hop neighbor of c and vice versa. However, because of a wormhole, q becomes a 2-hop neighbor of c. As shown in Fig.3, both ND_u and ND_c are $c's$ 1-hop neighbors. Suppose that q is in ND_v and not in ND_c and p is in ND_u. Because of the wormhole, there are $q \in N_1(p)$ and $p \in N_1(c)$. So $q \in N_2(c)$ holds. Therefore, q and c are 2-hop neighbors.

□

Corollary 1. *If there are 3 nodes, which are mutually non-1-hop neighbors, in the intersection of the neighbor sets of p and q where q and p are 2-hop neighbors, then p and q must be attacked by a wormhole.*

Proof. Without loss of generality, we assume that u and v are the wormhole nodes as shown in Fig.4. According to Theorem 2, any two nodes that are within communication range of the same wormhole are either 1-hop neighbors or 2-hop neighbors. Therefore, q and p are 2-hop neighbors. $C_1(p,q)$ includes the nodes within the overlapped area of CIR_p and CIR_q as well as ND_u. According to the definition of a hidden wormhole, the nodes in ND_u are 1-hop neighbors of the nodes in ND_v. However, there can be 3 nodes, e.g.(x,y,z), which are mutually non-1-hop neighbors within CIR_u. This contradicts Theorem 1. So, we draw the conclusion that p and q must be attacked by a wormhole.

□

5 Wormhole Detection and Isolation Algorithm

5.1 Overview

According to the Corollary 1, if 3 nodes occur, which are mutually non-1-hop neighbors, in the intersection of the neighbor sets of u and v where v and u are 2-hop neighbors, u and v are attacked by a wormhole. Thus, the problem of detecting wormholes is converted to the problem of identifying such a 3-node set in the intersection of the neighbor sets of the specific nodes. Therefore, we design a new wormhole detection and isolation algorithm. The algorithm works in a distributed manner. Each node in the network is equipped with the algorithm locally. Each node is also equipped with a neighbor information table as depicted in Table 1. The table records all 1-hop and 2-hop neighbors.

The wormhole detection and isolation (WDI) algorithm consists of four steps.

Table 1: A neighbor information table, where Node ID is the identification of a node; Neighbor Type ={1-hop neighbor, 2-hop neighbor}.

Node ID	Neighbor Type	Neighbor 1	Neighbor 2	...	Neighobr n

1. At the initial stage, every node discovers its 1-hop neighbors, and then broadcasts a message of "1-hop neighbors' information" to the nodes within 2 hops.

2. When a node receives "1-hop neighbors' information" messages from its neighbors within 2 hops, it records them into its neighbor information table.

3. Every node u runs the Lookup algorithm. It visits each node v in $u's$ 2-hop neighbor set to identify whether there are at least 3 nodes, which are mutually non-1-hop neighbors, in the intersection of the neighbor sets of u and v. If the Lookup algorithm finds such a 3-node set and returns TRUE, u then generates a list which includes all suspected nodes and broadcasts the list to its neighbors within 2 hops.

4. This step is selective. If the Lookup algorithm returns TRUE or wormhole notification messages are received, u launches the processing to remove all the suspected nodes from the network.

5.2 The Lookup Algorithm

As a key building block of our solution, the Lookup algorithm presents the way for any a node u to determine whether at least 3 nodes occur, which are non-1-hop neighbors, in the intersection of the neighbor sets of u and v.

Node u first computes $C_1(u,v)$, where v is a 2-hop neighbor of u, then randomly chooses a node i from $C_1(u,v)$. By removing i and $N_1(i)$ from $C_1(u,v)$, a new set $C_1(u,v) = C_1(u,v) - i - N_1(i)$ is obtained. If $C_1'(u,v)$ is not empty, u again randomly chooses a node j from $C_1'(u,v)$. By removing j and $j's$ 1-hop neighbors from $C_1'(u,v)$, $C_1''(u,v)$ is obtained.

Meanwhile, if $C_1''(u,v)$ is not empty, 3 nodes are found which are mutually non-1-hop neighbors. $Suspects(u)$ is set by computing the intersection of the neighbor sets among i, j and any node in $C_1''(u,v)$. If $C_1''(u,v)$ is empty, the above processing is repeated till $C_1''(u,v)$ is empty. If the return value is FALSE, it implies that there are no such 3 nodes.

Algorithm 1: The Lookup Algorithm

Result: To identify 3 nodes which are non-1-hop neighbors in the intersection of the neighbor sets of u and v.
input : u and v, where v and u are 2-hop neighbors.
output: If ≥ 3 non-1-hop neighbors are found, return TRUE and $Suspects(u)$. Otherwise, return FALSE.

```
1  BOOL Lookup(u, v, Suspects(u))
2  begin
3      foreach i ∈ C1(u, v) do
4          C1'(u, v) = C1(u, v) − N1(i) − i;
5          foreach j ∈ C1'(u, v) do
6              C1''(u, v) = C1'(u, v) − N1(j) − j;
7              if C1''(u, v) ≠ φ then
8                  Compute Suspects(u);
9                  return TRUE;
10             end
11         end
12     end
13     return FALSE;
14 end
```

5.3 WDI Algorithm

When u runs the WDI algorithm, it traverses $N_2(u)$ to find whether there are 3 nodes, which are mutually non-1-hop neighbors among $C_1(u,v)$ where v and u are 2-hop neighbors.

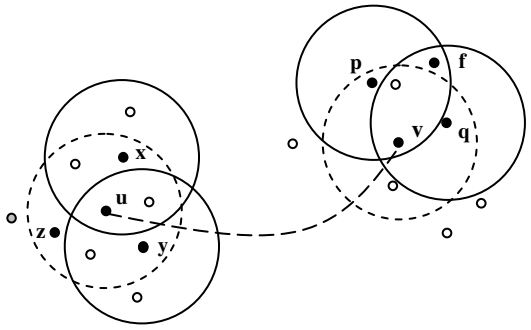
$Suspects(u)$ consists of two parts. One part is obtained by computing the intersection of the neighbor sets of u, v and any node in $C_1''(u,v)$, where v and u are 2-hop neighbors, as shown in the Lookup algorithm. The other part is obtained by computing the intersection of the neighbor sets of u and v. After that, a message of "wormhole notification" is generated according to $Suspects(u)$ and then broadcast to the nodes in $N_2(u)$. To ensure the reliability of the message, the notification message is signed with its private key.

Let's Revisit the scenario in Fig.4. When p executes the WDI algorithm, it traverses all the nodes in $N_2(p) = \{w, q, b, c, d, i, l, r\}$. Suppose that it chooses w from $N_2(p)$ first. After running the Lookup algorithm, it fails to find 3 nodes which are mutually non-1-hop neighbors among $C_1(p,w) = \{f\}$. So it chooses q from $N_2(p)$. It finds that there are 3 nodes $\{x, y, z\}$ which are non-1-hop neighbors from $C_1(p,q) = \{e, g, h, j, x, y, z\}$. Then p obtains $Suspects(p) = C_1(x,y,z) + C_1(p,q) = \{a, b, e, p, q, g, h, i, x, y, z\}$. P generates a "wormhole noti-

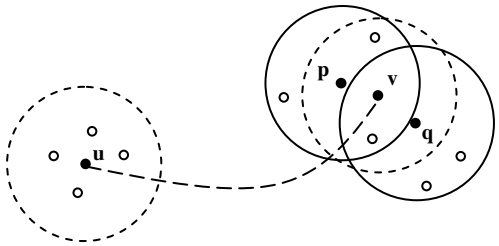
Algorithm 2: WDI - Wormhole Detection and Isolation Algorithm

Result: Executed by each node u to detect and isolate wormhole nodes from network.

```
1  void WDI()
2  begin
3      Suspects(u) = φ;
4      foreach i ∈ N2(u) do
5          if Lookup(u, i, Suspects(u)) then
6              add C1(u, i) to Suspects(u);
7              break;
8          end
9      end
10     if Suspcects ≠ φ then
11         generate wormhole notification message in
           terms of Suspects(u);
12         broadcast the message to N1(u) + N2(u);
13     end
14     receive wormhole notification message from
       i(i ≠ u);
15     remove Suspects(i) from N1(u);
16 end
```



(a) A scenario of false node alarm



(b) A scenario of miss detection alarm

Figure 5: The false node alarm and the miss detection alarm scenarios

fication" message and broadcasts it to $N_1(p) + N_2(p)$. The notification message is signed with $p's$ private key.

Some nodes, such as w and r, cannot judge whether they are attacked by a wormhole then. Fortunately, they can isolate a wormhole by receiving "wormhole notification" messages generated by other nodes, e.g. p. When r and w, which are in $N_2(p)$ but neither in $N_2(u)$ nor in $N_2(v)$, receive the "wormhole notification" message, they remove the nodes in $Suspects(p) = \{a, b, e, p, q, g, h, i, x, y, z\}$ from $N_1(r)$ and $N_1(w)$, respectively. They will not forward packets generated by the nodes in $Suspects(p)$.

Now, all the 2-hop neighbors of u, i.e. $\{c, d, f, i, l, r, w\}$, can obtain a list, which includes all the nodes that are directly attacked by a wormhole, i.e. $\{a, b, e, p, q, g, h, i, x, y, z\}$. Then, they remove all these attacked nodes from their 1-hop neighbor list. So the wormhole is isolated from the network after the above processing.

6 Performance Analysis

6.1 Miss detection and false alarm

According to the WDI algorithm, if the algorithm identifies at least 3 nodes, which are non-1-hop neighbors, in the intersection of the neighbor sets of u and v where u and v are 2-hop neighbors, u and v have been attacked by a wormhole. In order to isolate the wormhole, the WDI algorithm further removes the nodes, which are close enough to u and v. We have to point out that the WDI algorithm may suffer from both miss detection and false node alarm. Miss detection means that the wormhole attacks really exist but the WDI algorithm is not able to find them. False node alarm means that the WDI algorithm can correctly detect wormhole attacks but may recognize some clean nodes as nodes directly attacked by wormholes and falsely isolate them from the network. Fortunately, based on the corollary 1, the WDI algorithm does not cause any false detection alarms, which means if the WDI algorithm turns on an alarm, there must be a wormhole attack in the network.

Let's investigate the WDI algorithm again. We notice that the conditions to remove nodes in the WDI algorithm may mistakenly sacrifice some more nodes than necessary because the algorithm does not always distinguish clearly among potentially attacked nodes which in fact may be clean. As shown in Fig.5(a), f has been falsely suspected as being directly attacked by a wormhole. This leads to a false node alarm. In addition, the condition in the corollary is rather strict regarding the detection of wormhole attacks. Some wormhole attacks really exist but they do not satisfy the corollary 1, as shown in Fig.5(b). Because there are lower than 3 nodes, which are non-1-hop neighbors mutually, in the intersection of the neighbor sets of p and q,the lookup algorithm cannot identify wormhole attack. This

leads to a miss detection alarm. Therefore, in this section, we evaluate our solution regarding the miss detection ratio theoretically and the false node alarm ratio by simulation.

6.2 Detection probability analysis

Detection probability is inversely proportional to the miss detection alarm ratio, which is an important metric to evaluate wormhole detection algorithms. In this section, we compute the detection probability of the WDI algorithm. According to spatial statistics theory [17], under the randomly uniform deployment, the number of nodes within area $\Re$ satisfies the Poisson distribution. Given that ρ_g is the density of a network, the probability that there are k nodes within area $\Re$ is as follows:

$$P(\mid \Re \mid = k) \;=\; \frac{(\rho_g \Re)^k}{k!} e^{-\rho_g \Re} \tag{1}$$

Suppose that there are n nodes within CIR_u. The number of nodes within the area S ($S = \alpha\pi R^2$; α is the ratio of the area of S and the area of CIR_u) is calculated as follows:

$$\begin{aligned} P(\mid S \mid = k) &= \frac{(\rho_g S)^k}{k!} e^{-\rho_g S} \\ &= \frac{(\frac{n}{\pi R^2} \times \alpha\pi R^2)^k}{k!} e^{(-\frac{n}{\pi R^2} \times \alpha\pi R^2)} \\ &= \frac{(n\alpha)^k}{k!} e^{-n\alpha} \end{aligned} \tag{2}$$

Therefore, the probability that more than 1 node isolated in S is shown in formula (3).

$$P_S = P(\mid S \mid \geq 1) = 1 - P(\mid S \mid = 0) = 1 - e^{-n\alpha} \tag{3}$$

Fig.6 shows the relationship among P_S, n and α. Fig.7 illustrates the relationship between n and α when P_S ranges from 0.1 to 0.9. We observe that P_S increases as n or α grows. It implies that the higher degree of a node or the bigger area of a region, the higher probability that there is at least a node in the region. This is straightforward.

Now we consider the probability that there are 3 nodes which are non-1-hop neighbors. Suppose that the distance between u and v is d_{uv}, and d_{uv} is $2R$ as shown in Fig.8(a).

If node t is located in the shaded area, these three nodes, i.e., u, v and t, must be mutually non-1-hop neighbors and they are located in the same circle. The area of the shaded region is the same as in formula (4).

$$S_{shaded} = \pi R^2 - 2(2\pi R^2 \phi - Rdsin\phi) \tag{4}$$

where $\phi = cos^{-1}(\frac{d_{uv}}{2R})$ and $d_{uv} = R$. Hence, there is formula (5).

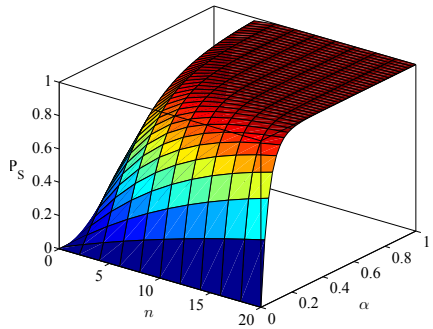


Figure 6: The relationship among n, α and P_S

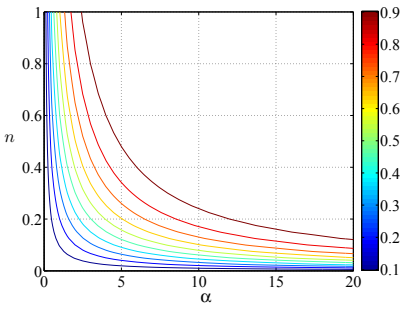


Figure 7: The relationship between n, α under certain P_S

$$S_{shaded} = \pi R^2 - 2(2R^2 cos^{-1}(\frac{1}{2}) - R^2 sin(cos^{-1}(\frac{1}{2}))) \tag{5}$$

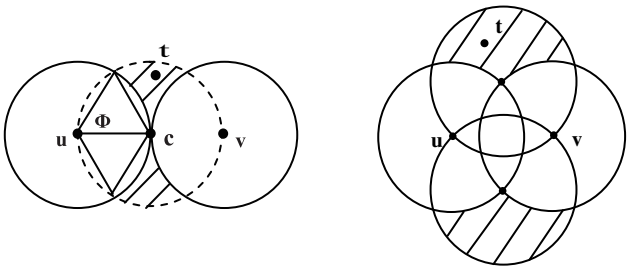
The ratio of the area of S and the area of CIR_u is represented by formula (6).

$$\alpha = \frac{S_{shaded}}{\pi R^2} = 0.218 \tag{6}$$

The probability that more than 1 node is located in the shaded area is as follows:

$$\begin{aligned} P_{shaded} &= P(\mid S_{shaded} \mid \geq 1) \\ &= 1 - P(\mid S_{shaded} \mid = 0) \\ &= 1 - e^{-0.218n} \end{aligned} \tag{7}$$

We illustrate the relationship between P_{shaded} and n in Fig. 9(a). If $d_{uv} \in (R, 2R]$ holds, as shown in Fig.8(b), the shorter d_{uv} is, the larger S_{shaded} and P_{shaded} are. Hence, in Fig.8(a) is the lower bound if there are 3 nodes that are non-1-hop neighbors.



(a) $d_{uv} = R$ (b) $d_{uv} \in (R, 2R]$

Figure 8: The probability of at least 3 non-1-hop neighbors in a circle

Table 2: Simulation Parameters

Parameter	Value
Area	100×100
Radio range	6
Placement	Uniform
Execution rounds	100

The detection probability of our approach P_{det} depends on the probability that there are 3 nodes which are non-1-hop neighbors on one side of a wormhole. Suppose that the probability that there are 3 nodes which are non-1-hop neighbors on one side of a wormhole is P_w. Therefore, the detection probability is $P_{det} = 1 - (1 - P_w)^2$. Under the uniform distribution, P_{shaded} reflects the probability that there are 3 nodes, which are mutually non-1-hop neighbors, in any circle. In other words, because the replaying radii of wormhole nodes are the same as those of the clean nodes, P_w is equal to P_{shaded}.

According to Fig.9(a) and 9(b), we observe that when the number of a node's average 1-hop neighbors approximates 10, the WDI algorithm's detection probability is close to 100%. It means that the miss detection alarm ratio is close to zero.

6.3 Simulation Setup

Our simulation has been carried on a custom-built, standalone C++ simulator. Various network scenarios are used to carefully analyze the performance of our approach. Our solution is only related to network topology and independent of the MAC and the Network Layers. The parameters for the simulation are shown in Table 2.

We have randomly deployed 400, 500, 600, 700, 800, 900, 1000, 1200, and 1400 nodes in a 100×100 area with node communication radii $R = 6$. We statistically work out that the corresponding average 1-hop neighbors are 4.3, 5.3, 6.3, 7.5, 8.4, 9.5, 10.5, 12.5, and 15, respectively, corresponding to each scenario. Fig.10(a) shows that the relationship between total node number and average 1-hop neighbors is almost linear.

6.4 Simulation Analysis

The WDI algorithm is run for 100 rounds in every scenario and calculates the averages of collected data. We focus our analysis on detection probability and false node alarm ratio, as well as communication overhead.

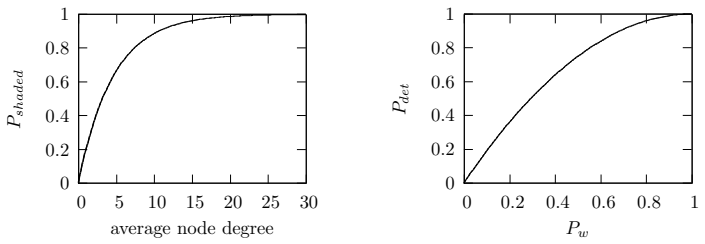
As shown in Fig.10(b), when a node's average 1-hop neighbors approximates 10, detection probability is close to 100. The reason is that with the increase of network density, it is more possible that there are 3 nodes which are non-1-hop neighbors on one side of a wormhole. Since our algorithm heavily depends on finding such an anomaly,the higher the degree a node is, the higher our detection probability is. Our approach is more suitable for a relatively dense network than for a sparse network. The plot is also consistent with our theoretical analysis in Section VI-A.

Fig.10(c) shows the relationship between the total number of wormhole notification messages and the number of average 1-hop neighbors. Although more notification messages will intensify network overhead, it can be alleviated by the use of message fusion. From another perspective, since notification messages are only broadcasted within 2 hop neighbors of the nodes directly attacked by a wormhole, the overhead is confined to a local area, and it will not significantly influence communication among other clean nodes. Therefore, we believe the side effects are trivial.

In Section VI-A, we pointed out that the WDI algorithm may suffer from false node alarms. Fig.10(d) shows the relationship between the false node alarm ratio and number of average 1-hop neighbors. We observe that our approach's false node alarm ratio is confined to 15%, even with the increase in network density. For example, if there are 20 nodes in the communication range of wormhole nodes, the WDI algorithm may excessively recognize 3 clean nodes as abnormal nodes and falsely isolate them from the network. The ratio is acceptable in practice. Meanwhile, the WDI algorithm will not cause a false detection alarm. This is also confirmed by the simulation.

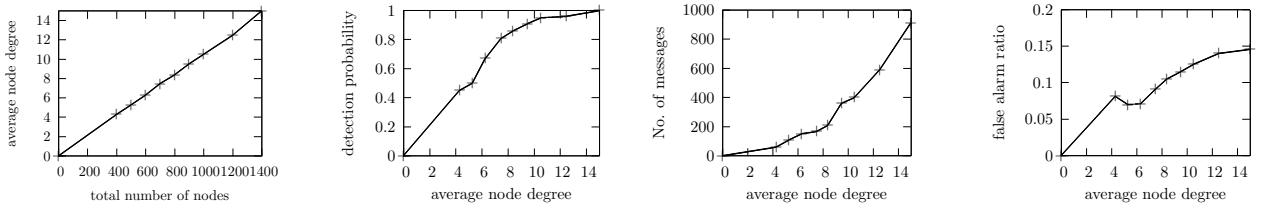
7 Conclusion

Wormhole attacks distort network topology, and degrade the performance of such applications like localization and data collection. A hidden wormhole is especially severe because it can be launched easily and be immune to cryptographic techniques. Existing approaches have limitations such as the need for GPS, time synchronization, and the burden of computation. We analyze and prove that when



(a) (b)

Figure 9: The relationship between (a) node degree and P_{shaded} and (b) P_w and P_{det}.



(a) # vs degree (b) Detection probability (c) # of notification messages (d) The ratio of false node alarm

Figure 10: The false node alarm and the miss detection alarm scenarios

average 1-hop neighbors are close to 10, it is highly possible that in an ad hoc network attacked by a wormhole, there are at least 3 nodes, which are non-1-hop neighbors, in the intersection of the neighbor sets of u and v where v and u are 2-hop neighbors. However, such phenomena will not be present in a normal topology. With this knowledge, we have designed a polynomial complexity algorithm to detect and isolate wormholes. Simulation results show that our approach performs well on detection probability, network overhead, false node alarms and miss detection alarms. Our approach now is under the UDG model. Further research will be done to improve and evaluate our approach under quasi-UDG models [18].

Acknowledgment

The research work is partially supported by the 973 Program under grant No: 2009CB320705 in China and and NSF China grant No: 60973122.

References

[1] B. Wu, J. Chen and J. Wu. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless Network Security, Part II, 2007, pp103-135.

[2] M. G. Zapata, and N. Asokan. Secure Ad hoc On-demand Distance Vector Routing. ACM Mobile Comp. and Commun. Review, Vol. 3, No. 6, 2002, pp106-07.

[3] K. Sanzgiri and B.Dahill. A Secure Routing Protocol for Ad hoc Networks. Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02), Paris, France, 2002, pp78-87.

[4] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. Proc. 8th ACM Int'l. Conf. Mobile Comp. and Net. (MOBICOM'02), Atlanta, Georgia, 2002, pp12-23.

[5] S. Buchegger and J. Le Boudec. Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad hoc Networks). Proc. 3rd Symp. Mobile Ad Hoc Net. and Comp. (MOBIHOC'02), New Orleans, Louisiana, 2002, pp226-236.

[6] L. Buttyan, and J. Hubaux. Security and Cooperation in Wireless Networks. Cambridge: Cambridge University Press, 2007.

[7] Y. Hu, A. Perrig, and D. Johnson. Wormhole Attacks in Wireless Networks. IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, 2006, pp370-380.

[8] R. Poovendran and L. Lazos. A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad hoc Networks. Wireless Networks, No.13, 2007, pp27-59.

[9] X. Wang, and J. Wong. An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks. 31st

Annual International Computer Software and Applications Conference (COMPSAC'07), Beijing, China, 2007, pp39-48.

[10] R. Maheshwari, J. Gao and S. Das. Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. Proc. 26th Ann. Joint Conf. IEEE Comp. and Comm. Societies (INFOCOM'07), Anchorage, Alaska, 2007, pp107-115.

[11] W. Wang, and B. Bhargava. Visualization of Wormholes in Sensor Networks. Proceedings of the 2004 ACM workshop on Wireless Security (WiSe'04), New York, NY, 2004, pp51-60.

[12] I. Khalil, S. Bagchi, and N. Shroff. MobiWorp: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks. Ad Hoc Networks, Vol. 6, No. 3, 2008. pp344-362.

[13] N. Song, L. Qian, and X. Li.Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach. 19th IEEE Int,l Parallel and Distributed Processing Symp. (IPDPS'05) - Workshop 17, Denver, Colorado, 2005, pp289-296.

[14] B. Clark, C. Colbourn, and D. Johnson. Unit Disk Graphs. Discrete Mathematics, Vol.86, Issue 1-3, 1990, pp165-177.

[15] A. Farago. Scalable Analysis and Design of Ad Hoc Networks via Random Graph Theory. Proceedings of the 6th Int'l Workshop on Discrete Algorithms and Methods for Mobile Comp. and Comm. Atlanta, Georgia, 2002, pp43-50.

[16] W. Wu, H. Du, and X. Jia et al. Minimum Connected Dominating Sets and Maximal Independent Sets in Unit Disk Graphs. Theoretical Computer Science, Vol. 352, Issues 1-3, 2006, pp1-7.

[17] N. Cressie. Statistics for Spatial Data. Revised edn. New York: Wiley, 1993.

[18] F. Kuhn, R. Wattenhofer, and A. Zollinger. Ad Hoc Networks beyond Unit Disk Graphs. Wireless Networks, Vol. 14, No. 5, 2007, pp715-729.

Appendix

Because the replaying radius of a wormhole node is important in our proposed approach, we discuss the replay radii of wormhole nodes further in detail. As far as we know, our discussion is the first complete analysis on such a topic.

As shown in Fig.11, u and v are wormhole nodes. We denote the dashed line circle centered at x with radius R by CIR_{R-x}. The real line circle centered at x with radius

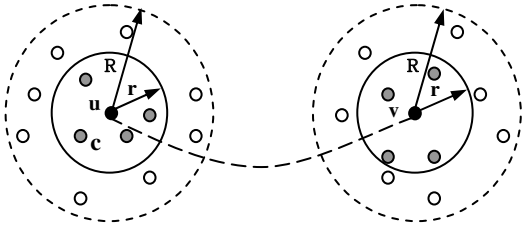


Figure 11: The communication area of a node affected by a wormhole

r is denoted by CIR_{r-x}. The nodes represented by small shaded circles on the x side are denoted by ND_{s-x}, while the nodes represented by hollow circles on the x side are denoted by ND_{h-x}.

Let's consider the behavior of the wormhole nodes first, especially their replaying radii. Wormhole node u can receive all the packets sent by the nodes within CIR_{R-u}. Limited by ranging accuracy, it cannot estimate the distance between itself and packet senders. So, it is wise for u to replay all the received packets to another wormhole node v. If v constrains its communication range within CIR_{r-v}, where $r < R$, only the nodes in ND_{s-v} can receive these packets. All ND_{s-v} nodes regard the nodes in CIR_{R-u} as their neighbors, but ND_{h-u} will not consider them as its neighbors because the nodes in ND_{h-u} cannot receive packets sent by these nodes. Thus, there are asymmetric links between ND_{s-v} and ND_{h-u}. It is the same for ND_{s-u} and ND_{h-v}. This contradicts the assumption of a bidirectional link. In addition, wormhole node u shouldn't only forward packets generated by part of nodes on the u side, e.g. node c, because all the nodes on the u side can overhear packets generated by the nodes on the v side when wormhole node u replays them to c. This also contradicts the bidirectional link. We conclude that in order to pretend to be clean nodes and not to be found easily, the wormhole nodes should usually have the same replaying radii as those of the clean nodes. They should also be able to transmit all the packets they receive.