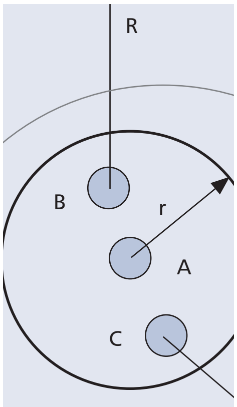
DETECTING WORMHOLE ATTACKS IN DELAY-TOLERANT NETWORKS

YANZHI REN, STEVENS INSTITUTE OF TECHNOLOGY
MOOI CHOO CHUAH, LEHIGH UNIVERSITY
JIE YANG AND YINGYING CHEN, STEVENS INSTITUTE OF TECHNOLOGY



The authors describe methods to detect wormhole attacks. However, most of them cannot work efficiently in DTNs. To detect the presence of a wormhole attack, they propose a detection mechanism that exploits the existence of a forbidden topology in the network.

ABSTRACT

Delay-tolerant networks are especially useful in providing mission-critical services including emergency scenarios and battlefield applications. However, DTNs are vulnerable to wormhole attacks, in which a malicious node records the packets at one location and tunnels them to another colluding node, which relays them locally into the network. Wormhole attacks are a severe threat to normal network operation in DTNs. In this article we describe various methods that have been developed to detect wormhole attacks. However, most of them cannot work efficiently in DTNs. To detect the presence of a wormhole attack, we propose a detection mechanism that exploits the existence of a forbidden topology in the network. We evaluated our approach through extensive simulations using both Random Way Point and Zebranet mobility models. Our results show that the proposed method can detect wormhole attacks efficiently and effectively in DTNs.

INTRODUCTION

Ad hoc networks can easily be deployed because they do not require fixed network infrastructures such as base stations or routers. Due to its self-organizing nature, an ad hoc network can be formed in real time where all participating nodes willingly perform packet forwarding for one another. Thus, ad hoc networks are flexible and can provide mission-critical services, especially in emergency applications and battlefield scenarios.

However, in practice, due to high node mobility, low node density, and short radio ranges, traditional ad hoc routing protocols do not work well in some challenging network scenarios as end-to-end paths may not always exist. For instance, nodes are sparsely connected in tactical fields for the search and rescue missions. To address this issue, the delay-tolerant network (DTN) concept [1] is introduced, which uses a store-and-forward approach to deal with challenging network scenarios. In DTNs nodes store packets if they cannot find a next-hop node to deliver them to destinations. New routing schemes have been designed for DTNs. For example, Prophet [2] requires that each node first stores packets in its memory and then selectively transmits packets when it encounters other nodes based on various metrics including the numbers of previous encounters, the last encounter time, and the estimated packet delivery probability values to other nodes.

In DTNs the portability of modern devices makes them tempting targets for thefts. Moreover, authenticated devices in chaotic battlefield environments are also likely to be captured by the enemy. Thus, it is easy for an adversary to compromise nodes within a DTN, and use these nodes to launch insider attacks. Such insider attacks can cause significant problems in networks. For instance, an adversary can use the compromised nodes to launch a particularly harmful attack called a wormhole attack [3]. In a wormhole attack the adversary connects two compromised nodes that are far away in the network using a low-latency link. Then, one compromised node records and tunnels data packets to another compromised node which replays them there. Such an action can give the nodes within the transmission range of the compromised nodes the impression that they are the neighbors of some other nodes that are actually far away. By creating such wormhole links between distant nodes, attackers can corrupt the topology views of the attacked networks, disrupt the routing in such networks, and significantly impact the normal operations of packet delivery. There has been active work developed in detecting wormhole attacks in ad hoc networks [3–6]. However, these methods have their limitations when applied to DTNs by either imposing rigorous requirements on resource-constrained nodes or relying on connectivity information, which is scarce in sparsely connected DTNs.

In this article we first give an overview of how a wormhole attack can be launched, its impact, and existing methods that have been developed to deal with this type of attack. Then we present the characteristics of DTNs and use Prophet as

1536-1284/10/$25.00 © 2010 IEEE

an example to describe routing in a DTN. We also describe how nodes in ad hoc networks typically move using two representative mobility models: the Random Way Point and Zebranet models.

Next, we describe a detection scheme we have designed, which only utilizes the network topology information for detecting a wormhole attack. In our scheme nodes in the network will reduce their transmission range for a short time period if necessary to detect the presence of a forbidden topology structure. Such a forbidden structure is caused by a wormhole attack and cannot be present under normal situations without attacks. Our detection mechanism does not require the deployment of additional devices in the DTNs. To show the effectiveness and efficiency of our detection scheme, we present simulation results by using a 40-node network running PROPHET. We examine the feasibility of our scheme for detecting wormhole attacks under various scenarios with different node densities and movement patterns. Finally, we present our concluding remarks.

Past Research on Countering Wormhole Attacks

Adversaries can launch a wormhole attack in various ways in ad hoc networks. For instance, attackers can compromise two nodes that are far apart and then build a direct link between them; attackers can also introduce two new nodes with transceivers that are compatible with the other nodes into the network and connect them using a direct link. This kind of direct link can be established using an out-of-band channel or a logical link via packet encapsulation. After the direct link is established, one end node can forward packets it receives from its neighbors to the other colluding end node via the wormhole link. The latter end node relays the received packets into the network.

A wormhole attack can heavily affect the network topology and hence disrupt the normal operation of routing protocols in ad hoc networks. Furthermore, the wormhole link can make the tunneled packets arrive with fewer hops compared with the packets transmitted over the normal routes. As a result, the malicious end nodes of the wormhole link may attract more routes through them. For example, when a wormhole attack is being launched against an ad hoc network running an on-demand routing protocol like Dynamic Source Routing (DSR) [7], the route request packets may be tunneled to the destination target node of the route request. The neighbors of the destination node will hear this request and discard all other received route request packets that arrive later. Thus, the wormhole attack can prevent any routes other than through the wormhole nodes to be discovered. Once the malicious nodes manage to force themselves to be part of the selected routes, they can then launch further attacks when they receive regular data traffic. For example, they can conduct selective data dropping, record the data for further traffic analysis, and so on. It is worth noting that it is relatively easy to launch a wormhole attack as the attacking nodes do not even need access to any cryptographic keys.

In order to detect wormhole attacks, some detection schemes have been proposed. For example, in [3] the authors added the location information from GPS into the transmitted packets. The receivers use the location information to verify whether there is a wormhole attack. This is referred to as the *geographical leash* approach in [3] and requires only loosely synchronized clocks. However, this method suffers when there are circumstances where obstacles prevent communication between two nodes that would otherwise be in the transmission range. The authors also proposed a temporal leash method where a sending node includes the time information in the packet and the receiving node compares the time at which it receives that packet to see if the packet has traveled beyond a threshold based on transmission time. However, this temporal leash approach requires tight clock synchronizations, and thus it is hard to achieve with resource-constrained nodes.

Reference [4] proposed the secure tracking of node encounters (SECTOR) scheme to prevent wormhole attacks. In SECTOR the Mutual Authentication with Distance Bounding (MAD) protocol enabled nodes to find their true neighbors by determining their mutual distances when they encounter one another. MAD used bit exchanges between each pair of encountered nodes: one node first sent out one bit, which is considered a challenge, and then another node responded with one bit immediately after receiving the challenge. By measuring the time between sending out a challenge and receiving the response, the first node can compute an upper bound of the distance between these two nodes and then check if this distance violates any physical constraints (e.g., the speed of light). The disadvantage of this method is that it needs special hardware for measuring timing with nanosecond precision.

In [5], the authors introduced directional antennas into a network and proposed a directional neighbor discovery protocol to prevent wormhole attacks. With directional antennas, the region around a node is divided into zones. Their neighbor discovery method is based on the fact that only nodes that are located in zones, which are in the opposite direction, can be true neighbors in legal networks. Thus, in this method the neighbor discovery protocol only allows nodes that are in certain zones to accept each other as neighbors, and this strategy can avoid accepting most of the fake neighbors masqueraded by the wormhole link. Even though this method greatly diminishes the threat of wormhole attacks, it requires all nodes to use directional antennas.

Another category of proposed methods is to use the network connectivity information for wormhole detection. For example, in [6] connectivity information is used to detect the presence of wormholes. However, these methods are not very effective when the networks become sparse because not enough connectivity information exists.

A wormhole attack can heavily affect the network topology and hence disrupt the normal operation of routing protocols in ad hoc networks. Furthermore, the wormhole link can make the tunneled packets arrive with fewer hops compared with the packets transmitted over the normal routes.

Traditional routing schemes designed for well-connected ad hoc networks do not work well in sparse ad hoc networks because they typically assume end to end paths exist between any pair of nodes. Thus, a new network architecture called delay tolerant network has been designed.

Our mechanism described in this article solely relies on detecting the presence of a forbidden topology structure in a DTN by utilizing the high mobility of the nodes as such structures cannot exist in legal networks. This approach works effectively in sparse networks and does not need any additional devices. Furthermore, this method can be applied in each node in a distributed manner, and hence is especially suitable in ad hoc networks.

Background

In this section we first provide an overview of DTNs and then illustrate the routing function in DTNs by using PROPHET as an example. We also describe how nodes typically move around in ad hoc networks by presenting two mobility models: Random Way Point and Zebranet.

Delay Tolerant Network

Wireless ad hoc networks may be sparsely connected due to low node density (i.e., too few nodes spreading across a large geographical area). Traditional routing schemes designed for well connected ad hoc networks do not work well in sparse ad hoc networks because they typically assume that end-to-end paths exist between all pairs of nodes. Thus, a new network architecture, the DTN, has been designed to allow nodes with intermittent connectivity to communicate with one another. Nodes in a DTN are expected to store data packets in persistent storage when they cannot find any next hop nodes to forward the data packets. In addition, a custodian feature is provided such that a node will not remove a data packet from its storage until it can find another downstream node willing to be the custodian of this data packet. Furthermore, a late binding feature is also defined for nodes in a DTN such that data packets can be sent using descriptive names; for example, a message is meant for all faculty members within Lehigh University who are currently located within 500 m of the Packard Laboratory.

New routing schemes have been designed for DTNs [8]. DTN routing schemes can be divided into three categories:

1 Routing schemes that utilize specially deployed nodes called *message ferries*

2 Routing schemes that make use of history-based information to estimate delivery probability of peers and pass the message to the peer that can best deliver the message

3 Routing schemes that use two-hop relay forwarding where a source can send multiple copies to different relay nodes and have the relay nodes deliver to the destination when they encounter the destination

In this article, we use PROPHET, which belongs to category 2, as an example to illustrate the routing function in a DTN.

Overview of PROPHET

PROPHET [2] is a routing protocol proposed for DTNs, which uses history of node encounters and transitivity. In this probabilistic routing scheme, a probabilistic metric $P(a,b)$ called delivery probability is established at each node a for each known destination node b. This metric indicates how likely it is that node a could deliver a message to node b. A node will forward data to another node it encounters if that node has a higher delivery probability to the destination than itself.

In PROPHET three equations are used to update the delivery probability values. Node a will update its metric whenever it encounters another node b using Eq. 1:

$$P(a,b) = P(a,b)_{\text{old}} + (1 - P(a,b)_{\text{old}}) \times \alpha, \qquad (1)$$

where α is an initialization constant set to 0.75. If a pair of nodes a and b do not encounter each other for a time period, node a updates its delivery probability to node b using Eq. 2:

$$P(a,b) = P(a,b)_{\text{old}} \times \gamma^{k}, \qquad (2)$$

where γ is the aging constant. For example, γ is set to 0.98. k is the number of beacon periods from the last encounter between nodes a and b. In addition, the delivery probability also has a transitive property: when node a encounters node b, which encountered node c previously, node a will update its delivery probability to node c based on the delivery probabilities of $P(a,c)$ and $P(b,c)$ using Eq. 3:

$$\begin{aligned} P(a,c) = {} & P(a,c)_{\text{old}} + (1 - P(a,c)_{\text{old}}) \\ & \times P(a,b) \times P(b,c) \times \beta, \end{aligned} \qquad (3)$$

where β is a scaling constant (e.g., $\beta = 0.25$) that controls the impact the transitivity value has on the delivery predictability. In this article, we use the PROPHET routing protocol in our simulation to evaluate the performance of our forbidden-topology-based detection mechanism.

Mobility Models

Typically, a mobility model is used to describe how nodes move in ad hoc networks. We refer to mobility models where the nodes move in the same manner as homogeneous mobility models, and mobility models where nodes may move differently as non-homogeneous mobility models. The Random Way Point (RWP) mobility model is the best-known homogeneous mobility model that researchers often use to compare different ad hoc routing schemes. However, the RWP mobility model may not reflect the node movements often seen in real-world scenarios. Thus, researchers construct new mobility models based on traces collected from real networks. For example, Zebranet [9] is an ad hoc sensor network deployed in Africa where small wireless sensor nodes are attached to zebras, and the movements of zebras are indirectly obtained from the contact traces of the attached wireless sensor nodes. A mobility model constructed from these real Zebranet traces is referred to as the Zebranet mobility model. While other mobility models exist, RWP and Zebranet are two representative mobility models; one is a homogeneous mobility model representing ideal situations, while the other captures the node movement scenarios in real-world environments. In this article we study the effectiveness of our wormhole detection scheme under these two mobility models.

Random Way Point — Reference [7] introduced the RWP mobility model. In this mobility model each node selects a random destination and moves to that destination at a speed uniformly distributed between zero and the maximum speed. After reaching the destination, the node pauses for a fixed period before selecting another destination and repeating the process as previously described until an experiment duration ends.

Zebranet — As described earlier, the Zebranet model is constructed based on contact traces collected from a real ad hoc sensor network deployed in Africa. This model is constructed as follows. Each node independently selects a speed and turning angle every 3 min, and the values of the speed and turning angle are chosen from distributions that match traces collected from real movements of zebras. The speed and turning angle selection processes are repeated for the whole experimental study duration. Compared to the RWP model, the nodes in the Zebranet model move faster, and the movements are more chaotic.

Detecting Wormhole Attacks via Forbidden Topology

Detecting wormhole attacks is important in DTNs because they can significantly disrupt network delivery performance, which relies heavily on the normal operations of ad hoc routing protocols. We develop a simple, yet effective, wormhole attack detection mechanism in which nodes reduce their transmission range for a short period of time to check for the existence of any forbidden topology in a network to determine the existence of the wormhole attacks.

Communication Model

We use the unit disk graphs (UDG) model described in [6] as the communication model between nodes in DTNs. In such a communication model each node uses an omnidirectional antenna. Thus, the transmission range of each node is modeled as a disk of unit radius in the plane. All nodes located within a node's disk are neighbors of this node.

Forbidden Topology

We illustrate our wormhole attack detection mechanism by describing the forbidden topology, which is the foundation of our mechanism. We denote the neighbor sets of a node i as $N(i)$. Furthermore, if a node B can receive packets from node A, node B is a neighbor of node A and satisfies $B \in N(A)$. The basic idea of the *forbidden topology* is to examine the network topology by exploiting the geometric relationship of nodes' locations under the constraint of the transmission range of a node.

We illustrate this idea in Fig. 1 by studying the geometric relationship among nodes A, B, and C. Both nodes B and C are neighbors of node A. When the transmission range of A is R, it is possible that the distance between nodes B and C is larger than R. However, when the transmission range of A is reduced to r with $r < R/2$, there is a constraint of the distance between B and C when keeping both of them as neighbors of node A.

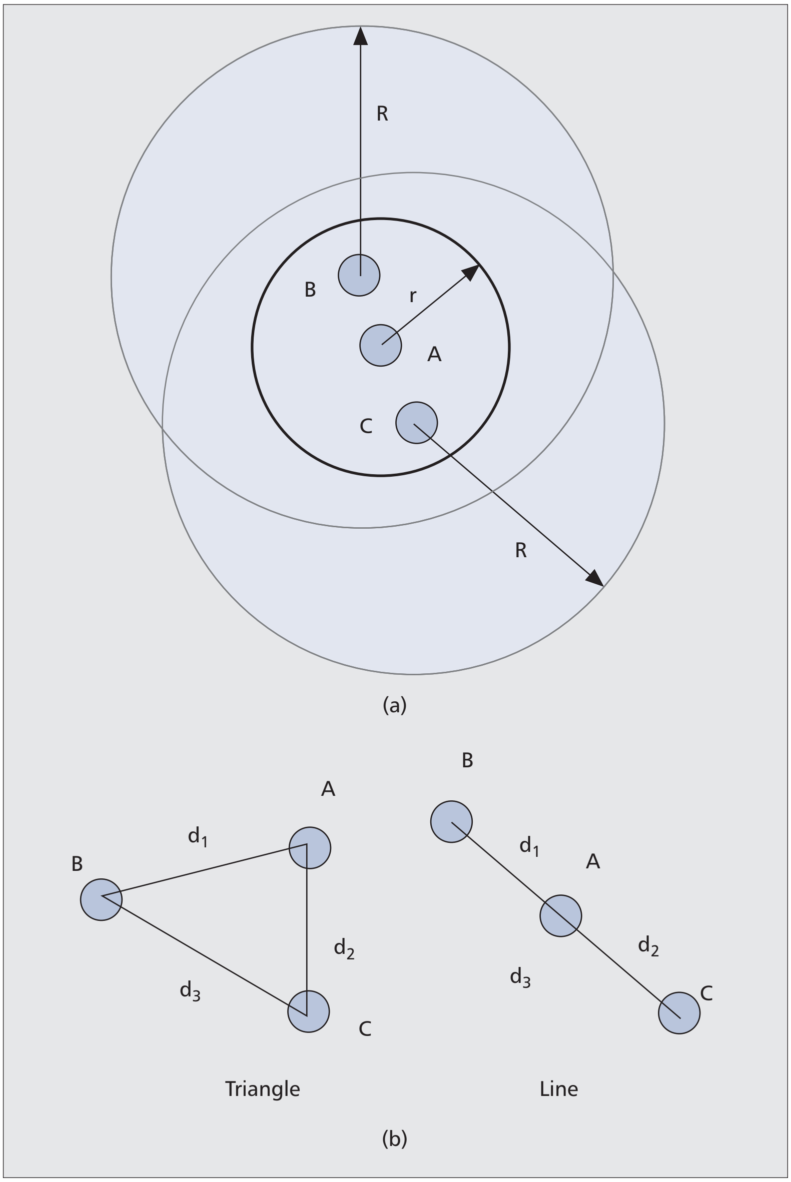


Figure 1. *Illustration of a forbidden topology: a) example of a forbidden topology; b) two different node placements.*

We study this distance constraint as follows. Let us denote the distance between nodes A and B as d_1; the distance between nodes A and C as d_2; and the distance between nodes B and C as d_3. There are only two possible ways to place these three nodes in a network topology, *triangle placement* or *line placement*, as depicted in Fig. 1. In the triangle placement, since both nodes B and C are neighbors of node A, nodes B and C are both in transmission range of node A (i.e., $d_1 \le r < R/2$ and $d_2 \le r < R/2$). Therefore, $d_1 + d_2 < R/2 + R/2 = R$. Since nodes A, B, and C form a triangle, we also have $d_1 + d_2 > d_3$ based on the triangular law. Thus, we obtain $d_3 < R$. This indicates that the distance between nodes B and C cannot be larger than R. On the other hand, in the line placement we have $d_1 + d_2 = d_3$. We can also obtain $d_3 = d_1 + d_2 < R/2 + R/2 = R$.

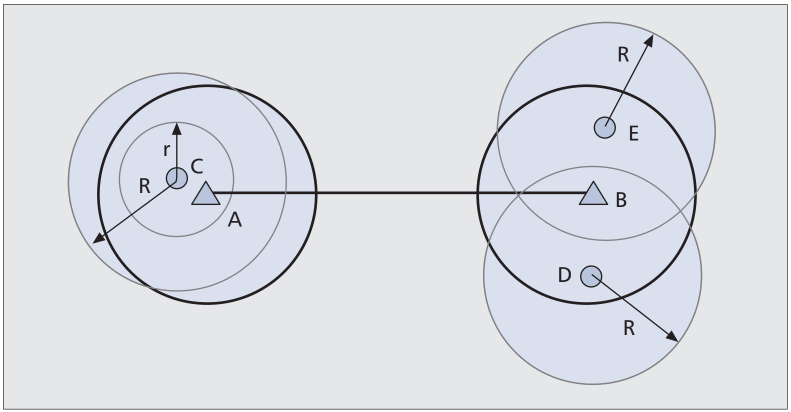


Figure 2. *Detecting a wormhole attack via the forbidden topology.*

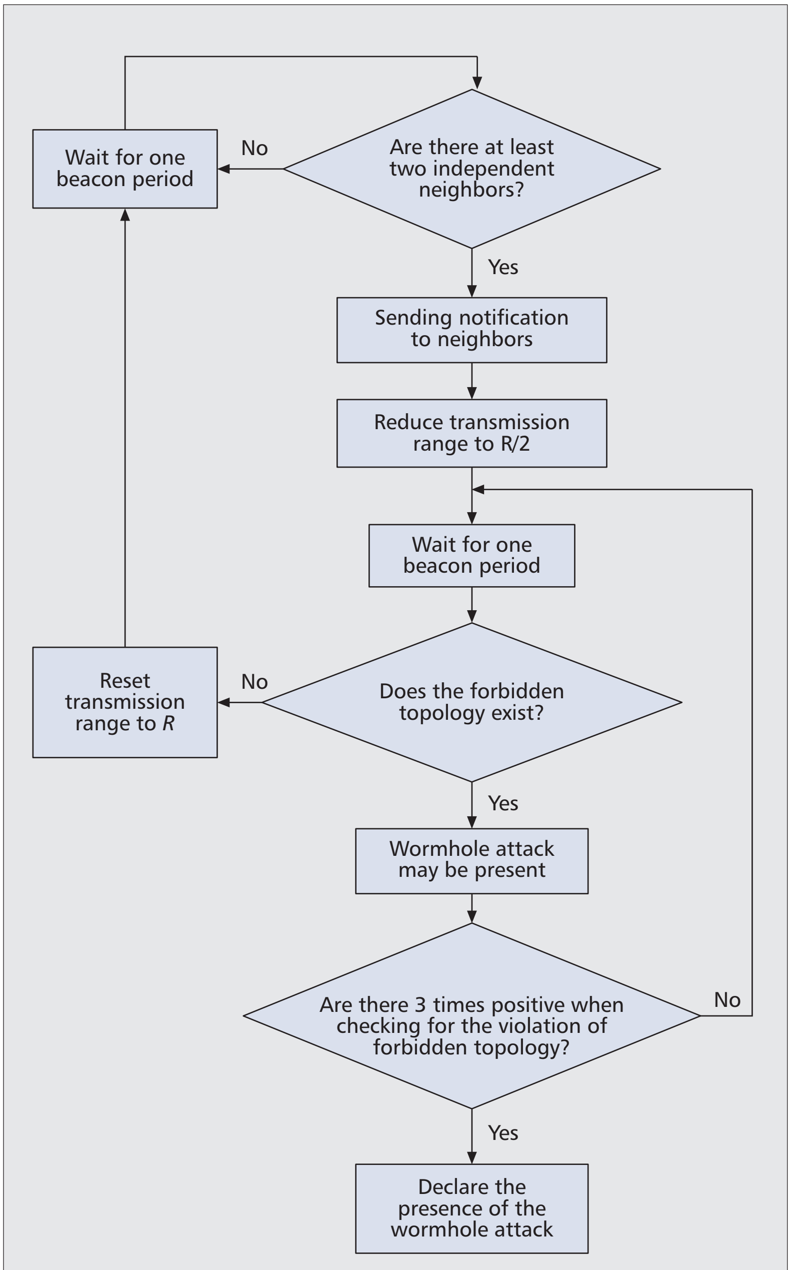

Wait for one beacon period
No
Are there at least two independent neighbors?
Yes
Sending notification to neighbors
Reduce transmission range to R/2
Wait for one beacon period
Reset transmission range to *R*
No
Does the forbidden topology exist?
Yes
Wormhole attack may be present
Are there 3 times positive when checking for the violation of forbidden topology?
No
Yes
Declare the presence of the wormhole attack

Figure 3. *Flow of the attack detection process by exploiting the forbidden topology.*

Thus, we obtain an important observation: if the radius of node A's transmission range is r and the transmission range of other nodes (e.g., B and C) is R with $r < R/2$, it is impossible to have $B \in N(\mathrm{A})$ and $C \in N(\mathrm{A})$; however, $B \notin N(C)$ or $C \notin N(B)$. In other words, if both nodes B and C are neighbors of node A, node B must be a neighbor of node C and vice versa.

Detection Philosophy

The forbidden topology is the foundation for diagnosing the existence of a wormhole attack. As depicted in Fig. 2, when a wormhole attack is present, nodes A and B are compromised by an adversary who launches the wormhole attack. Because of the wormhole attacks launched by nodes A and B, nodes D and E are both neighbors of node C (i.e., $D \in N(C)$ and $E \in N(C)$). However, $D \notin N(E)$ or $E \notin N(D)$. Thus, node C has two independent neighbors: nodes D and E. Independent neighbors are two nodes that are not in each other's neighbor lists. Node C then reduces its transmission range. If node C still finds two independent neighbors after reducing the transmission range, a forbidden topology has been identified, suggesting the presence of a wormhole attack. On the other hand, during normal situations, nodes D and E are not neighbors of node C. Then no forbidden topology can be found.

Example

A detailed description of our detection mechanism for wormhole attacks may be found in [10]. Using node C as an example, we show the main steps of diagnosing the presence of a wormhole attack via the identification of any forbidden topology as follows. The flow chart of the detection steps is depicted in Fig. 3. We assume that each node (e.g., node C) keeps its current neighbor list $N(C)$, and this list can be maintained by exchanging delivery information when the node (e.g., node C) encounters other nodes. In addition, each node can request to obtain the neighbor lists of its neighbors. This can be done by adding the neighbor list to periodic beacon messages. Since a DTN is a sparse network, the number of neighbors of each node is small. Thus, the incurred communication cost is low.

Node C searches through its neighbor list and determines whether there are at least two independent neighbors. If two independent neighbors exist, node C starts the procedure of detecting the wormhole attack. Node C first includes a message in its beacon to notify all the nodes in $N(C)$ that it will reduce its transmission range. All nodes that receive this notification will not change their transmission range in the next beacon time. After node C sends out this message, it reduces its transmission range from R to r where $r < R/2$. If no two independent neighbors exist, node C starts searching again through its neighbor list from the next beacon time.

Once node C reduces its transmission range to r, it updates $N(C)$ and searches through its neighbor list again. If there are still at least two independent neighbors, the forbidden topology is violated, and node C declares the presence of a wormhole attack. However, if there are no

Distance between wormhole nodes (meters)	500	700	900	1100	1300	1500
Average detection time (seconds)						
3000 m × 3000 m, RWP	473	538	545	553	607	833
2000 m × 2000 m, RWP	139	138	127	183	206	248
3000 m × 3000 m, Zebranet	297	309	264	382	409	460
Detection rate						
3000 m × 3000 m, RWP	0.84	0.82	0.8	0.83	0.82	0.83
2000 m × 2000 m, RWP	0.92	0.91	0.91	0.92	0.91	0.9
3000 m × 3000 m, Zebranet	0.85	0.85	0.89	0.85	0.9	0.87
False positive rate						
3000 m × 3000 m, RWP	0	0	0	0	0	0
2000 m × 2000 m, RWP	0	0	0	0	0	0
3000 m × 3000 m, Zebranet	0.0067	0.0053	0.0026	0.0070	0.0052	0.0052

Table 1. *Simulation results under different distances between wormhole nodes.*

The effectiveness of our forbidden-topology-based detection mechanism can be evaluated through detection rate and false positive rate. Overall, we found that the detection rate is higher under a denser network.

more than two independent neighbors after the reduction of transmission range, node C resets its transmission range back to R and starts searching again in the next beacon time.

In order to improve the detection accuracy, the presence of a wormhole attack can be declared after n times when a node (e.g., node C) detects the violation of the forbidden topology. Additionally, reducing the transmission range to $r = R/2$ helps to capture the violation of the forbidden topology in a timely manner.

Detection Efficiency

Our first evaluation is to measure the efficiency of our forbidden-topology-based detection mechanism. It is defined as the time it takes for the first node to detect the existence of the forbidden topology and declare the presence of a wormhole attack.

To show the generality of our approach, we present results of several simulated experiments conducted with NS2. We tested using three scenarios with varying node densities and different movement patterns of the nodes: 3000 m × 3000 m RWP, 2000 m × 2000 m RWP, and 3000 m × 3000 m Zebranet.

Table 1 presents the average detection time as a function of the distance between two nodes launching wormhole attacks. We observed that higher node density results in faster detection of a wormhole attack. Furthermore, the detection time increases as the distance between two wormhole nodes increases. This is because when the distance between the wormhole nodes becomes larger, the wormhole nodes will get closer to the boundary of the simulation environment, where fewer nodes located. As a result, it needs more time to detect the presence of the forbidden topology and consequently determine the existence of a wormhole attack. We call this phenomenon the *boundary effect*.

Turning to examine the detection time under different node movement patterns, we found that the detection time in Zebranet (Table 1) is shorter than that in RWP. This is because under Zebranet, the nodes' movements are faster and more chaotic. Therefore, the probability that the nodes detect the presence of a forbidden topology increases, and as a result it takes shorter time to detect a wormhole attack. The statistical behavior of the detection time, presented as the cumulative distribution function (CDF) of the detection time in Fig. 4, shows the consistent observation as the average detection time.

Effectiveness of Detection

The effectiveness of our forbidden-topology-based detection mechanism can be evaluated through detection rate and false positive rate. We studied the detection rate as a function of the distance between the wormhole nodes under three simulation scenarios. Overall, we found that the detection rate is higher under a denser network. This is because when the network is denser, there is a higher probability of detecting the presence of the forbidden topology. Additionally, the detection rate under Zebranet is higher than that under RWP. As the nodes in Zebranet have higher mobility than in RWP, it is easier to detect the presence of the forbidden topology and thus determine the existence of a wormhole attack.

By looking at the false positive rate when detecting wormhole attacks, Table 1 shows that the false positive rate of our scheme is zero for RWP and less than 1 percent for Zebranet.

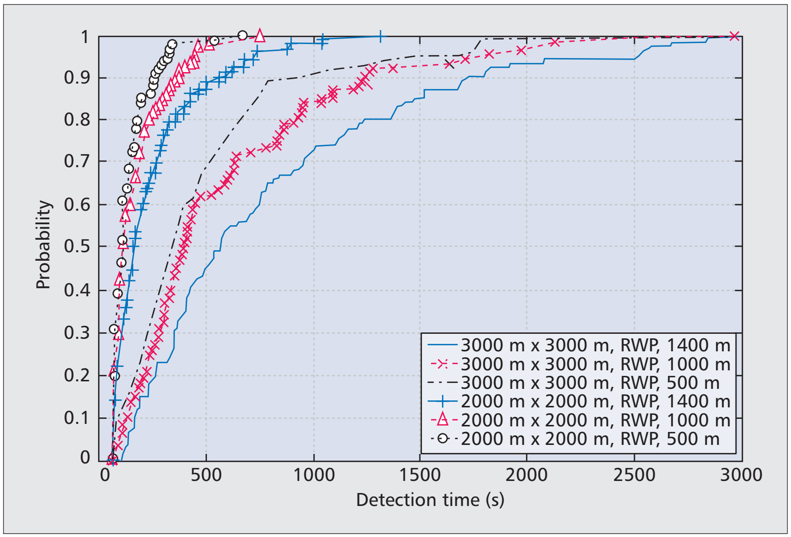


Figure 4. *CDF of the detection time when varying the distance between two wormhole nodes.*

Because Zebranet has higher mobility than in RWP and the beacon periods are not synchronized for all the nodes, it is possible that some nodes do not have the chance to update their neighbor list, although they move into the transmission range of the node that has reduced its transmission range. Overall, these observations suggest that our proposed approach is effective in detecting the presence of wormhole attacks.

Conclusion

Wormhole attacks are especially harmful in disrupting the normal network operation in DTNs. We describe the current work on detecting wormhole attacks in ad hoc networks. However, most of them either require special hardware or are not applicable to DTNs. We propose a detection mechanism that utilizes the determination of the presence of a special network topology, which is forbidden in a network under normal situations without attacks, by reducing the transmission range of a node for a short time period during detection. This detection mechanism is fully distributed and does not require any special hardware. Extensive simulations are conducted under two representative mobility models, Random Way Point and Zebranet, to evaluate both the efficiency and effectiveness of the detection mechanism.

References

[1] S. Farrell and V. Cahill, *Delay and Disruption Tolerant Networking*, Artech House, 2006.

[2] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic Routing in Intermittently Connected Networks," *ACM SIGMOBILE Mobile Comp. Commun. Rev.*, 2003.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," *Proc. IEEE INFOCOM*, 2003.

[4] S. Capkun, L. Buttyan, and J. P. Hubaux, "Sector: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks," *Proc. ACM SASN*, 2003.

[5] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," *Network Distrib. Sys. Sec.*, 2003.

[6] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information," *IEEE INFOCOM*, 2007.

[7] J. Broch *et al.*, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *Proc. 4th ACM/IEEE MobiCom*, 1998.

[8] Z. Zhang and Q. Zhang, "Delay/Disruption Tolerant Mobile Ad Hoc Networks: Latest Develops," *Wireless Commun. Mobile Comp.*, vol. 7, no. 10, May 2007.

[9] P. Juang *et al.*, "Energy-Efficient Computing for Wildlife Tracking: Design Trade-Offs and Early Experiences with Zebranet," *Proc. ASPLOS*, 2002.

[10] Y. Ren *et al.*, "Mitigation Schemes Against Wormhole and Blackhole Attacks in Delay Tolerant Networks," tech. rep., Stevens Inst. of Tech., Nov. 2009.

Biographies

Yanzhi Ren (yren2@stevens.edu) received his B.S. and M.S. degrees in June 2005 and June 2008, respectively, from the University of Electronic Science and Technology of China, Chengdu. He is currently working toward a Ph.D. degree in the Electrical and Computer Engineering Department at Stevens Institute of Technology. His research interests include the areas of information security and privacy.

Mooi Choo Chuah [SM] (chuah@cse.lehigh.edu) received her M.S. and Ph.D. degrees in electrical engineering from the University of California, San Diego. After her Ph.D., she spent 12 years at Bell Laboratories where she conducted research related to wireless system design, mobility, and resource management in wireless networks and the Internet, and other areas. She has been awarded 58 U.S. patents and eight international patents in these areas. Since 2004 she has been at Lehigh University where she works on designing next-generation wireless networks, network security, and mobile social networks. She is currently a member of Sigma Xi.

Jie Yang (jyang@stevens.edu) received his B.E. degree in automatic control from Beijing Institute of Technology, China, in 2004. He was in a Ph.D. program in the Department of Automatic Control of Beijing Institute of Technology from 2005 to 2007. He is currently working toward a Ph.D. degree in the Electrical and Computer Engineering Department at Stevens Institute of Technology. His research interests include the areas of information security and privacy, wireless localization, and location-based services.

Yingying Chen (yingying.chen@stevens.edu) received her Ph.D. degree in computer science from Rutgers University. She is currently an assistant professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her research interests include wireless and system security and privacy, wireless networking, and distributed systems. She coauthored the book *Securing Emerging Wireless Systems*, and has published extensively in journal and conference papers. Prior to joining Stevens Institute of Technology, she was with Bell Laboratories and the Optical Networking Group, Lucent Technologies. She received the IEEE Outstanding Contribution Award from IEEE New Jersey Coast Section each year, 2005–2009. She is the recipient of the NSF CAREER award. She is also the recipient of the Best Technological Innovation Award from the International TinyOS Technology Exchange in 2006, as well as the Best Paper Award from the International Conference on Wireless On-demand Network Systems and Services (WONS) in 2009.