Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks

Dezun Dong, *Member, IEEE*, Mo Li, *Member, IEEE*, Yunhao Liu, *Senior Member, IEEE*, Xiang-Yang Li, *Senior Member, IEEE*, and Xiangke Liao

***Abstract*—Wormhole attack is a severe threat to wireless ad hoc and sensor networks. Most existing countermeasures either require specialized hardware devices or make strong assumptions on the network in order to capture the specific (partial) symptom induced by wormholes. Those requirements and assumptions limit the applicability of previous approaches. In this paper, we present our attempt to understand the impact and inevitable symptom of wormholes and develop distributed detection methods by making as few restrictions and assumptions as possible. We fundamentally analyze the wormhole problem using a topology methodology and propose an effective distributed approach, which relies solely on network connectivity information, without any requirements on special hardware devices or any rigorous assumptions on network properties. We formally prove the correctness of this design in continuous geometric domains and extend it into discrete domains. We evaluate its performance through extensive simulations.**

***Index Terms*—Connectivity, topological approach, wireless ad hoc and sensor networks, wormhole detection.**

I. Introduction

WORMHOLE attack is one of the most severe security threats [1]–[15] in ad hoc and sensor networks. In wormhole attacks, the attackers tunnel the packets between distant locations in the network through an in-band or out-of-band channel. The wormhole tunnel gives two distant nodes the illusion that they are close to each other. The wormhole can attract and bypass a large amount of network traffic, and thus the attacker can collect and manipulate network traffic. The attacker is able to exploit such a position to launch a variety of attacks, such as dropping or corrupting the relayed packets, that significantly imperils a lot of network protocols including routing [3], [7], localization, etc. [16]. This paper focuses on typical wormhole attacks. The adversary is an outsider who does not have valid network identity. The establishment of wormhole attacks is independent of the general security mechanisms employed in the network. The attacker can forward each bit of a communication stream over the wormhole directly without breaking into the content of packets. Thus, the attacker does not need to compromise any node and obtain valid network identities to become part of the network. Using the wormhole links, the attacker is able to gather enough packets and exploit the wormhole attack as a stepping stone for other more sophisticated attacks, such as man-in-the-middle attacks, cipher breaking, protocol reverse engineering, etc. Wormhole attacks have posed a severe threat to wireless ad hoc and sensor networks.

Many countermeasures have been proposed to detect wormholes in wireless ad hoc and sensor networks. Those solutions typically catch the attacks by detecting partial symptoms induced by wormholes. Generally, existing symptom-based methods either depend on specialized hardware devices or make relatively strong assumptions on the networks. For example, some approaches employ specialized hardware devices, such as GPS [3], [6], directional antennas [4], or special radio transceiver modules [10], which introduce significant amounts of extra hardware costs for the systems. Other types of approaches are based on ideal assumptions, such as global tight clock synchronization [3], special guard nodes [8], attack-free environments [11], or unit disk communication models [9]. These requirements and assumptions largely restrict their applicability in networks composed of a large number of low-cost resource-constrained nodes.

To fully address wormhole attacks in ad hoc and sensor networks, we need to answer the following two questions: 1) what symptoms feature the most essential characteristics caused by wormhole attacks; and 2) how to gracefully design the countermeasures without critical requirements or assumptions. Our design goal is to rely solely on network connectivity information to detect and locate the wormholes. We focus our study on a fundamental view on the multihop wireless network topologies, aiming at catching the topological impact introduced by the wormhole. More concretely, we explore the fact that a legitimate multihop wireless network deployed on the surface of a geometric terrain can be classified as a 2-manifold surface of genus 0, while the wormholes in the network inevitably introduce singularities or higher genus into the network topology. We classify wormholes into different categories based on their impacts on topology. We then design a topological approach, which captures fundamental topology deviations and thus locates the wormholes by tracing the sources leading to such ex-

Manuscript received October 07, 2009; revised May 16, 2010 and November 18, 2010; accepted March 29, 2011; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor D. Agrawal. Date of publication August 22, 2011; date of current version December 16, 2011. The work of D. Dong was supported in part by the NSFC under Grants 60903223 and 60903224. This work of M. Li was supported by COE_SUG/RSS_20Aug2010_13/14 in Nanyang Technological University of Singapore. The work of X.-Y. Li was supported in part by NSF CNS-0832120 and NSF CNS-1035894.

D. Dong and X. Liao are with the School of Computer and the National Laboratory for Paralleling and Distributed Processing, National University of Defense Technology (NUDT), Changsha 410073, China (e-mail: dong@nudt.edu.cn; xkliao@nudt.edu.cn).

M. Li is with the Computer Science Division, School of Computer Engineering, Nanyang Technological University, Singapore 639798, Singapore (e-mail: limo@ntu.edu.sg).

Y. Liu is with the TNLIST, School of Software, Tsinghua University, Beijing 100084, China, and also with The Hong Kong University of Science and Technology, Kowloon, Hong Kong (e-mail: liu@cse.ust.hk).

X.-Y. Li is with Department of Computer Science, Illinois Institute of Technology, Chicago, IL 61606 USA (e-mail: xli@cs.iit.edu).

Digital Object Identifier 10.1109/TNET.2011.2163730

ceptions. Our approach solely explores the topology of the network connectivity and can be carried out in a distributed manner. We do not require any special hardware devices, yet have no additional assumptions on the networks, such as awareness of node locations, network synchronization, unit disk communication model, or special guard nodes. Although node density impacts on the detection performance of the method, our method works well in networks with fair node densities, which is verified by our simulations.

The rest of this paper is organized as follows. We first discuss those existing studies in Section II, and then formally define the wormhole problem and its detection methods in Section III. Section IV characterizes the wormholes in topologies and describes theoretical principles of a fundamental detection method. Section V presents our topological detection approach in discrete networks. We evaluate this work through comprehensive simulations and analysis in Section VI. Finally, we conclude this work in Section VII.

II. Related Work

Existing countermeasures largely rely on observing the derivative symptoms induced by wormholes residing in the network. All of these approaches have their respective advantages and drawbacks. Applicability of approaches is largely dependent on specific system configurations and applications.

Some approaches observe the symptom of Euclidean distance mismatch in the network. Hu *et al.* [3] introduce geographic packet leash. By appending the location information of the sending nodes in each packet, they verify whether the hop-by-hop transmission is physically possible and accordingly detect the wormholes. Wang *et al.* [6] instead verify the end-to-end distance bounds between the source and the destination nodes. Zhang *et al.* [17] propose a location-based neighborhood authentication scheme to locate the wormholes. Such approaches require the preknowledge of node locations to capture the distance mismatch.

Some approaches observe the symptom of time mismatch in packet forwarding. Hu *et al.* [3] introduce temporal packet leash, which assumes tight global clock synchronization and detects wormholes from exceptions in packet transmission latency. Capkun *et al.* [10] propose SECTOR, which measures the round-trip travel time (RTT) of packet delivery and detects extraordinary wormhole channels. SECTOR eliminates the necessity of clock synchronization, but assumes special hardware equipped by each node that enables fast sending of one-bit challenge messages without CPU involvement. Eriksson *et al.* propose another RTT based approach, TrueLink [7].

Some approaches observe the symptom of neighborhood mismatch that leads to physical infeasibility. Hu *et al.* [4] adopt directional antennas and find infeasible communicating links by utilizing the directionality of antenna communication. Khalil *et al.* [11] propose LiteWorp, which assumes the existence of an attack-free environment before the wormhole attacks are launched. During the deployment phase, each node collects its 2-hop neighbors, and LiteWorp then selects guard nodes to detect wormhole channels by overhearing the infeasible transmissions among nonneighboring nodes. They further propose MobiWorp [12] to complement LiteWorp with the assistance of some location-aware mobile node.

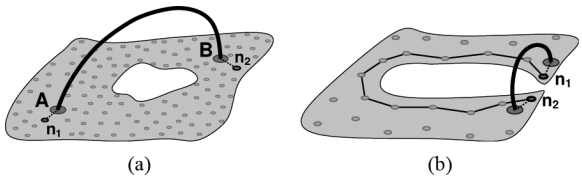


Fig. 1. Two examples of wormhole attack. (a) One typical wormhole. (b) Another wormhole, where geometric distance between wormhole endpoints does not correctly reflect the network communication path.

Some approaches observe the symptom of graph mismatch under special assumptions of network graph models. Poovendran *et al.* [8] present a graph-based framework to tackle wormholes. Their approach assumes the existence of guard nodes with extraordinary communication range. Wang *et al.* [5] graphically visualize the presence of wormholes. They reconstruct the layout of the networks by a centralized multidimensional scaling (MDS) to capture the wrap introduced by wormholes. Authors in [9] exploit the forbidden packing number in the unit disk graph (UDG) and propose a completely localized approach to detect wormholes with only network connectivity. It may fail when connectivity graphs do not follow the UDG model or a wormhole does not cause an increase of packing number.

Some approaches observe the symptom of traffic flow mismatch based on statistic analysis on the network traffic. Song *et al.* [13] observe the fact that the wormhole links are selected for routing with abnormally high frequency, and by comparing with normal statistics, they can identify the wormhole links. Another statistical approach proposed by Buttyan *et al.* [14] captures the abnormal increase of the neighbor number and the decrease of the shortest path lengths due to wormholes. The base station then centrally detects wormholes using hypothesis testing based on prestatistics of normal networks.

III. Problem Formulation

In this section, we present the wormhole attack model and system assumptions. We formulate the generalized wormhole problem with network connectivity.

A. Assumptions and Attacker Model

We consider a collection of homogeneous nodes deployed over a surface of terrain. Each node performs the homogeneous transmission control and is only capable of communicating with adjacent nodes in its proximity. We do not force a UDG communication model. We assume that the coordinates of nodes are unavailable. In wormhole attacks, the attackers tunnel the packets between distant locations in the network through a high-speed out-of-band channel. Fig. 1(a) displays a classic example of a wormhole attack. The attacker's link is referred to as a *wormhole link* or simply a *wormhole*. The two ends of a wormhole link are *wormhole endpoints*. In this example, AB represents a wormhole link in the network connecting two distant areas. The adversary can capture and replay the packet signals in the physical layer or simply retransmit the packet in the link layer [3]. In

this case, as illustrated in Fig. 1(a), nodes n_1 and n_2 can communicate directly as if they were direct neighbors.

We make the common assumptions on wormhole attacks, which are widely adopted in most previous wormhole countermeasures [3]–[9]. Wormhole attacks are defined based on the minimum capabilities required by the attacker to perform these attacks. In particular, the attacker does not need to compromise any node or have any knowledge of the network protocol used. Wormhole endpoints deployed by the adversary do not have valid network identities and do not become part of the network. The adversary launches *outsider* wormhole attacks in the network. We assume that in the network exist mechanisms that authenticate legitimate nodes and establish secure links between authenticated nodes. The communications can be protected by lightweight symmetric-key or asymmetric cryptographic mechanisms for sensor networks in link and upper layers [18], [19]. Although wormhole attacks impact neighboring discovery mechanisms in the physical or link layer greatly, transmitted data over encrypted network protocols remain transparent and unobservable to the wormhole attacker, as formulated in most previous works [3]–[9].

B. Connectivity-Based Wormhole Problem

Poovendran *et al.* give a formal definition of the wormhole problem based on the UDG communication graph model in Euclidean space [8]. According to their definition, a communication link is a wormhole link if the distance between its two endpoints exceeds the regular communication range. Their definition naturally binds the wormhole features with external geometric environments, and thus neglects the inherent topological impacts introduced by wormholes. For example, consider the network shown in Fig. 1(b). The Euclidean distance between nodes n_1 and n_2 can be very little and even within the maximum possible communication range of the two nodes, but they simply cannot directly communicate due to the obstacle or disturbance between them. Hence, the current shortest communication path between nodes n_1 and n_2 in the network is a long journey, denoted as the black lines in Fig. 1(b). If the external bold-line link is inserted into the network connecting n_1 and n_2, the two nodes are then able to communicate directly, and the shortest path between them is shortened remarkably. Obviously, in this case a wormhole attack occurs, but it is not covered by the definition in [8] because the distance between nodes n_1 and n_2 does not exceed the maximum communication range. We hereby present a more general and fundamental definition of the wormhole attack based only on network topologies.

Definition 1 (Generalized Wormhole Attacks): Let G be a communication graph of a network, and w be an attack on the network. Let G_w be the perceived communication graph after the attack w. Let $L(u,v)$ and $L_w(u,v)$ denote the lengths of the shortest paths between an arbitrary pair of nodes $u, v \in V(G) \cap V(G_w)$ on G and G_w, respectively. If $L_w(u,v) < L(u,v)$, we say that G_w is under wormhole attacks (or w launches a wormhole attack). $\lambda_{uv} = L(u,v) - L_w(u,v)$ quantifies the shortened path length of w between u and v. The intensity of the wormhole attack w is defined as $\lambda = \max\{\lambda_{uv} | u, v \in V(G) \cap V(G_w)\}$.

Definition 1 formalizes the wormhole attack based only on the network topologies. The wormholes defined by Poovendran *et al.* are indeed all included by our definition. The attack intensity λ describes the intensity of the topological distortion brought by the wormhole attack. Intuitively, a larger λ corresponds to a more intensive distortion on network topologies.

An ideal wormhole detection method should require as little preknowledge assumptions about the network as possible. The only preknowledge that we will assume is the fact that the network is deployed on a continuous geometric surface (2-manifold), where each node locally communicates with neighboring ones.

IV. Characterizing Wormholes

In this section, we model and characterize wormhole attacks on network topologies in continuous domain. We first characterize the topological features of wormholes and classify the wormholes. We then present the principles for the wormhole detection and prove theoretical guarantees. We extend our discussion to practical discrete networks in Section V.

A. Preliminaries

We use concepts and terminologies in combinatorial and computational topology. We first give a brief overview on the concepts and theories involved in our later discussions. Not all definitions are necessarily standard. For detailed explanations, please refer to those topology books [20].

In our paper, we consider network deployment region as connected, compact, and orientable (two-sided) 2-manifold *surfaces*, where each point has a neighborhood homeomorphic either to the plane or to the closed half-plane. This definition contains almost all ordinary surfaces observable in our daily life. In the rest of the paper, all *surfaces* mean such surfaces unless we explicitly state otherwise. Given two topological spaces X and Y, two continuous maps $f, g : X \rightarrow Y$ are said to be *homotopic* if there exists a continuous map $F : X \times I \rightarrow Y$ such that $F(x,0) = f(x)$ and $F(x,1) = g(x)$ for all $x \in X$, $I = [0,1]$. Any such mapping F is called a *homotopy* connecting f and g. Two curves with the same endpoints on the surface are homotopic to each other if and only if one can be smoothly deformed to the other without leaving the surface. A closed curve is *contractible* if it is homotopic to a point, otherwise it is *noncontractible*. A closed curve is *nonseparating* if the surface keeps connected after its removal. A closed curve is *separating* if it splits the surface into two or more components. The genus of a surface represents the maximum number of simple closed curves that can be removed without disconnecting the manifold. For example, a sphere and a disc have genus 0, while a torus has genus 1. Homotopy establishes an equivalence relation on the set of closed curves on a surface with any fixed basepoint. It classifies the set of cycles on a given surface into a set of homotopy classes, where cycles in each class are transformable to one another while cycles in different classes are not.

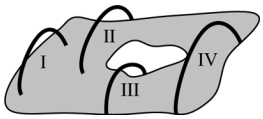


Fig. 2. Four different types of wormholes on the surface.

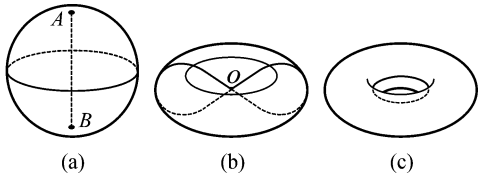


Fig. 3. (a) Link AB glued on a spherical surface X. (b) Link AB is contracted to a single point O. (c) Torus Y, which may collapse into $X\backslash AB$ by contracting a longitudinal cycle into one point.

B. Characterizing Wormholes

Normally, a wireless multihop network is deployed on the surface of a geometric environment, such as a plane or a rough terrain. In this section, we develop principles in continuous domain, assuming continuous deployment of nodes over the geometric surface with one-to-one mapping to the points on the surface. In the continuous setting, a legitimate network is a 2-manifold surface without singular points and of genus 0, which is homotopic to the plane area with a certain number of boundaries (holes). We refer to the surface of the legitimate network as *original surface*. A wormhole link is a continuous line segment with extremely short length that connects two points on the surface.

A new topology space is formed after the wormhole is glued on the original surface. We subsequently analyze how the different topology spaces are generated after gluing different types of wormholes. We classify wormholes into four categories, according to their topological impacts. Fig. 2 shows the four types of wormholes. For the Class-I wormhole, both of its endpoints are located inside the surface. The Class-II wormhole has one endpoint inside the surface and the other on the boundary of the surface. The Class-III wormhole has its endpoints on two different boundaries. The Class-IV wormhole has both of its endpoints on the same boundary. The four types of wormholes have different topological impacts on the original surface, and the complex wormhole attack can be considered as a finite combination of them. We first consider the impact of a single wormhole. We then analyze the impact of the combination of multiple wormholes.

1) Single Wormhole Impact: In this section, we analyze the impact of a single wormhole in different types, from Class I to IV. The main results are presented in Theorem 1.

Theorem 1: After inserting one wormhole into the original surface, the Class-I or Class-II wormhole adds one degenerated genus, the Class-III wormhole adds one genus and reduces a boundary, and the Class-IV wormhole adds a boundary.

Class-I and Class-II Wormholes: Fig. 3 shows an example of how a spherical surface X is affected by a wormhole link AB, which represents a Class-I or Class-II wormhole. Fig. 3(a) shows the new topology quotient space $X\backslash AB$ [20], with link AB glued on the spherical surface X. Fig. 3(b) shows a homotopy-equivalent topology with Fig. 3(a), which contracts the line AB into a single point O. The new topology space can be considered as collapsed from a torus Y, as shown in Fig. 3(c). By contracting a longitudinal cycle around the torus, Y collapses into $X\backslash AB$. Clearly, such a collapse is not a homotopy equivalence from Y to $X\backslash AB$. In this sense, we say that $X\backslash AB$ contains degenerated genus 1. Strictly speaking, the new topology space after the injection of a Class-I or Class-II wormhole is no longer a surface, as the neighborhood of the wormhole endpoint is not homeomorphic with a plane or closed half-plane. Informally, we call it a surface with singularities.

Class-III Wormholes: When the surface is of multiple boundaries (the network containing physical holes), a Class-III wormhole might appear as shown in Fig. 4(a). The topology space of Fig. 4(a) is homotopy-equivalent to that in Fig. 4(b), which contracts the wormhole link into a point. We focus on the two noncontractible cycles α and β in Fig. 4(b). Cycle α goes through the wormhole, and cycle β wraps the inner boundary. Fig. 4(b) can be seen as the deformation retract of Fig. 4(c), where the cycles α and β in Fig. 4(c) correspond to α and β in Fig. 4(b), respectively. Indeed, Fig. 4(a)–(c)is homotopy-equivalent to each other. Typically, a Class-III wormhole concatenates two different boundaries and increases the genus by 1. An interesting phenomenon happens under a Class-III wormhole. The twisted cycle α and cycle β are actually symmetrical to each other in the sense of topology. If we overturn the surface in Fig. 4(c), the meridional circle α becomes a longitudinal circle, while the longitudinal circle β becomes a meridional circle. Without the knowledge that β is homotopic to a physical boundary beforehand, we are not able to differentiate α and β in Fig. 4(b) through only topologies.

Class-IV Wormholes: A Class-IV wormhole connects two points on the same boundary. Thus, a Class-IV wormhole adds a bridge to the original surface and separates the boundary into two.

In summary of above discussions, we obtain the Theorem 1.

2) Combination of Multiple Wormholes: When two or more wormholes exist on the surface, Class-I or Class-II wormholes still introduce independent impacts, each leading to the increase of degenerated genus by 1. Multiple Class-III and Class-IV wormholes, however, might introduce interchangeable effects. As the example shown in Fig. 4(d), two Class-IV wormholes w_1 and w_2 are injected on the surface crossing each other. A single wormhole w_1 or w_2 adds a boundary to the surface, but the combination of them adds genus by 1. As a matter of fact, Fig. 4(d) is homotopy-equivalent to Fig. 4(a)–(c). The example above can be explained as follows. After the first Class-IV wormhole w_1 or w_2 is glued on the surface, the boundary of the original surface is split into two. When we add the second Class-IV wormhole, its two endpoints are then on two different boundaries, so the wormhole is slid to a Class-III wormhole to the new surface. The consequence is a combination of a Class-IV wormhole and a Class-III wormhole, leading to the increase of genus.

When multiple wormholes are injected to the original surface, we can consider them as being sequentially glued to the surface. The type of each wormhole is determined according to

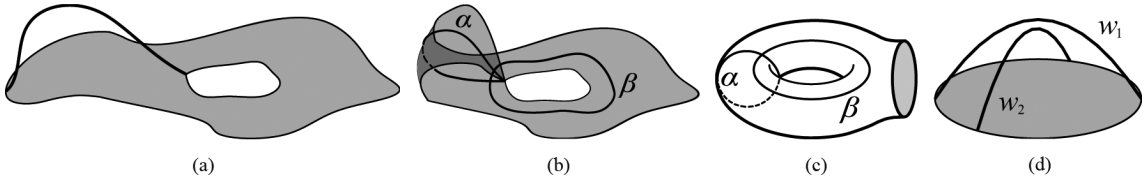


Fig. 4. Iimpact of wormholes. (a) Single Class-III wormhole. (b) Homotopic surface when contracting the wormhole link in (a). (c) Homotopic surface to (a) and (b). (d) Two Class-IV wormholes crossing each other.

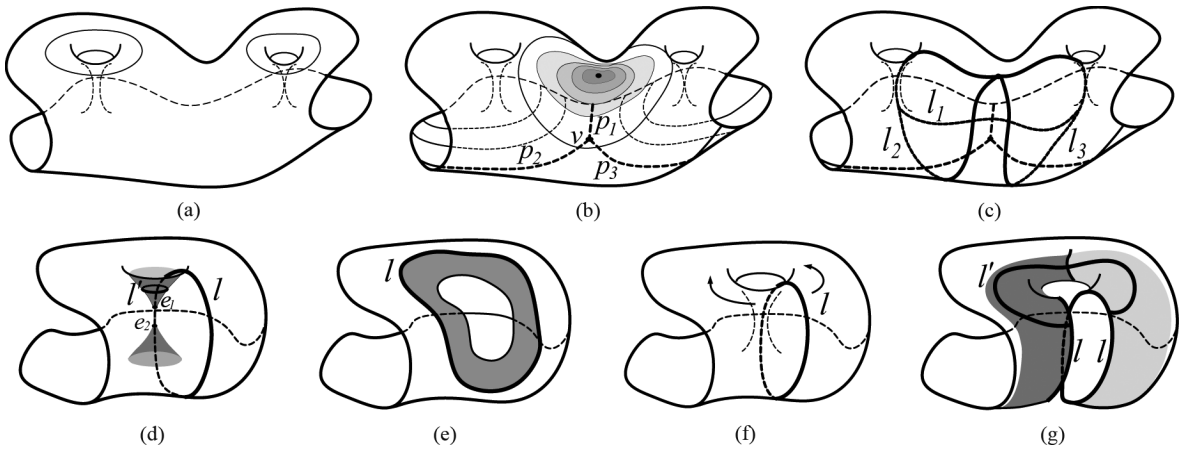


Fig. 5. Tracing wormholes by topologies. (a) Wormhole infected surface. (b) Shortest geodesic paths and cut locus. (c) Candidate loop set. (d) Locating Class-I or Class-II wormholes. (e) Separating loop formed by plain holes. (f) Nonseparating loop introduced by Class-III or Class-IV wormholes. (g) Detecting knit nonseparating loop pair.

the instant surface when it is glued. Class-I and Class-II wormholes will not be affected by previous injected wormholes, while Class-III and Class-IV wormholes might interchange their types according to the boundary separation or concatenation. The sequence in gluing the wormholes does not affect the final topological impact. We look into the final impact of multiple wormholes and characterize the topology surface with genus g, degenerated genus d, and b boundaries as $\tau(g, d, b)$, where g, d, and b are nonnegative integers. We can obtain the Theorem 2, which can be proved by following Theorem 1 and induction on the number of wormholes.

Theorem 2: Given the original surface $\tau_0 = \tau(g_0, d_0, b_0)$ and the final surface $\tau(g, d, b)$ after N wormholes are injected, there is $N = 2(g - g_0) + (d - d_0) + b - b_0$. Among the N wormholes, there are $d - d_0$ Class-I or Class-II wormholes and $2(g - g_0) + b - b_0$ Class-III or Class-IV wormholes.

According to our preknowledge on the legitimate network graph, the original surface has genus 0 and degenerated genus 0, so the original surface can be characterized as $\tau(0, 0, b_0)$, where b_0 is the number of boundaries (which is equal to the number of inner holes $+1$). According to Theorem 2, we can calculate the number of different types of wormholes if we can characterize the final topology space.

C. Tracing Wormholes

We hereby present the principle of tracing wormholes in continuous topology surface. For the convenience of presentation, we take a macroscopic view on the global network. We use an example of a surface with wormholes shown in Fig. 5 to explain this design. The proposed algorithm aims to trace wormholes through detecting the genus and degenerated genus. The main idea of the algorithm is to find the nonseparating cycles associated with wormholes. Two circular lines in Fig. 5(a) indicate two potential nonseparating cycles in this example.

1) Finding Cut Locus and Candidate Loops: Given the wormhole infected surface S, we first select an arbitrary point in S as the root and run a continuous *Dijkstra* shortest-path algorithm [21], as shown in Fig. 5(a). Each point is thereafter aware of its shortest geodesic paths to the root. We call the set of points that have more than one shortest path to the root the *cut locus* [21], denoted by C_S. After discovering the *Dijkstra* shortest paths to the root, we find a cut locus forms there. If we cut the surface along the cut locus, the surface becomes a topological disk. The paths marked by bold dashed lines are part of the cut locus. The point in the cut locus that has at least three shortest paths to the root is called a *branch vertex* of the cut locus, like point v in Fig. 5(b). The branch vertices separate the cut locus into *cut paths*, like paths p_1, p_2, and p_3 in Fig. 5(b). Each cut path has two endpoints. The endpoint of a cut path can be a branch vertex or not. We call the endpoint a *leaf vertex* if it is not a branch vertex. The leaf vertex can be on the boundary or in the interior of the surface. We further distinguish them as a *boundary leaf vertex* and *interior leaf vertex*. We can transform the cut locus C_S into its subgraph *reduced cut locus* through repeatedly removing all interior leaf vertices [21]. We denote the obtained reduced cut locus as $C(P, V)$, where P is the set of cut paths and V is the set of branch and boundary leaf vertices.

Let $p \in P$ be a cut path in the reduced cut locus and $a \in p$ be an arbitrary point on p. There are at least two nonhomotopic

shortest paths from a to the root. By concatenating the two nonhomotopic paths, we obtain a loop l_a, and it is clear that loop l_a is noncontractible. We say that a is the witness of l_a. For any two points $a, b \in p$, if l_a and l_b are the loops witnessed by a and b, respectively, l_a and l_b are homotopy-equivalent [21]. For each cut path $p \in P$, we arbitrarily select a loop witnessed by one point p and denote it as l_p. Thus we obtain a set of loops $L = \{l_p | \, p \in P\}$, which we call the *candidate loop set*. Fig. 5(c) displays the three candidate loops l_1, l_2, and l_3, corresponding to the three cut paths p_1, p_2, and p_3 in Fig. 5(b), respectively. Following [22, Lemma 4.2], there are at most $4(g+d)+2b-2$ branch vertices and $6(g+d)+3b-3$ cut paths. Hence, the number of candidate loops $|L| < 6(g+d)+3b-3$. For each candidate loop $l \in L$, we do the following steps to clarify the situations of wormholes.

2) Locating Class-I or Class-II Wormholes: To begin with, for checking whether or not the loop passes through a degenerated genus (Class-I or Class-II wormholes), we consider a small closed ε-neighborhood $N(l)$ of l. $N(l) = \{\varepsilon(x) | \, x \in l\}$, where $\varepsilon(x)$ denotes the ε-neighborhood of point x on the surface. As shown in Fig. 5(d), the bold line denotes the candidate loop l, which passes through a Class-I wormhole with its two endpoints labeled as e_1 and e_2. If there exists a sufficiently small simple closed curve l' in $N(l)$ that crosses l odd times (two curves are not crossed if they touch [20]), l can be marked as a loop through the Class-I or Class-II wormhole. We call l an *independent nonseparating loop*. We can further contract the cycle l' in the figure as much as possible while keeping it crossing l odd times. The cycle l' eventually contracts to one endpoint of the wormhole, i.e., node e_1 in Fig. 5(d). By this means, we can detect the endpoints of all Class-I and Class-II wormholes.

3) Detecting Class-III or Class-IV Wormholes: The case of Class-III and Class-IV wormholes is different. As both endpoints of such wormholes are on the boundaries of a surface, we cannot find such a small cycle enclosing each endpoint of a wormhole. Instead, we directly detect the genus by checking whether the candidate loop l is a separating or nonseparating loop. There is an essential difference between the two types of loops. The separating loop is two-sided, but the nonseparating loop is one-sided. Fig. 5(e) displays a separating loop that is formed due to the plain holes on the surface. It is two-sided in the sense that if we flood from the loop with different colors, e.g., the two colors never meet. The loop shown in Fig. 5(f), however, is a nonseparating loop formed by genus. If we flood light gray and dark gray to its two sides, as shown in Fig. 5(f) and (g), the two colors ultimately meet with each other because the loop is one-sided. By detecting the nonseparating loop l, we detect the genus introduced by Class-III or Class-IV wormholes. Let t be a point on the cut between the two color areas. Let $s \in l$ be an arbitrary point on l. There is a pair of nonhomotopic paths from s to t, one across the area of one color and the other one across the other color area. The two paths form a loop, which we denote in Fig. 5(g) as l'. Apparently, l' crosses l at a single point s. As we will later see in Lemma 4, both l and l' are nonseparating loops. We call l a *dependent nonseparating loop* and l' the *partner loop* of l. Furthermore, we call the two nonseparating loops that cross each other a *knit nonseparating loop pair*. We can conclude that there must be at least one Class-III or Class-IV wormhole in the knit nonseparating loop pair. Yet, as we mention in Fig. 4(c), the two loops are topologically indistinguishable, and we cannot conclude which loop passes through the wormhole.

To summarize, for each candidate loop $l \in L$, we classify it into one of the three types: separating loop, independent nonseparating loop, or dependent nonseparating loop. We detect and locate Class-I and Class-II wormholes from independent nonseparating loops. We detect Class-III and Class-IV wormholes from dependent nonseparating loops.

D. Correctness and Optimality

We prove that our method is able to detect all the detectable wormholes correctly. We first discuss the correctness and capability of this method, and then analyze the theoretical bound in topologically detecting wormholes.

Theorem 3: Let L be the set of candidate loops; all wormholes reside within L.

Proof: It is not difficult to prove that there exists a subset $L' \subseteq L$, which constitutes a homotopy basis of the original surface [21]. Let w be an arbitrary wormhole on the surface, and l_w is an arbitrary loop on the surface that passes through w. Since L' is a homotopy basis, there must exist a loop l_c homotopy-equivalent to l_w while l_c can be represented as the concatenation of some proper loops in L'. It means w must be passed through by at least one loop in $L' \subseteq L$. ■

From Theorem 3, we have confined the locations of all possible wormholes within the candidate loops L, although we may not be able to locate exactly the endpoints of all wormholes on L. Now, we prove our method is effective and accurate on detecting Class-I and Class-II wormholes. We first present Lemma 4, which follows [23, Lemma 2.1] and reveals the parity property of the nonseparating loops.

Lemma 4: On surface S, a cycle c is nonseparating if there is a cycle c' such that c' crosses c odd times.

Theorem 5: All Class-I and Class-II wormholes are detected and exactly located by our method.

Proof: Let w be an arbitrary Class-I or Class-II wormhole. According to Theorem 3, there exists a loop $l_w \in L$ that passes through w. Since w is a Class-I or Class-II wormhole, w increases one degenerated genus on the surface. For the degenerated genus, there exists a contractible simple closed curve at one end of the genus that crosses l_w one time, i.e., all Class-I and Class-II wormholes can be effectively detected without false negative. On the other hand, let l be an arbitrary loop in L. If there exists a contractible loop l' in the ε-neighborhood of l crossing l oddly, according to Lemma 4, l must be nonseparating. l' is both nonseparating and contractible, so l' is continuously deformed and contractible to an endpoint of at least one degenerated genus, never otherwise. When ε is sufficiently small, it guarantees that there is only one endpoint inside l'. Thus, the detection method accurately locates the Class-I and Class-II wormholes. ■

Theorem 6: Let l and l' be a pair of knit nonseparating loops. There is at least one Class-III or Class-IV wormhole on l and l'.

Proof: Suppose that neither l nor l' passes a wormhole, then l and l' are also loops on the original surface without wormholes. Since l and l' form a knit nonseparating loop pair, l and l'

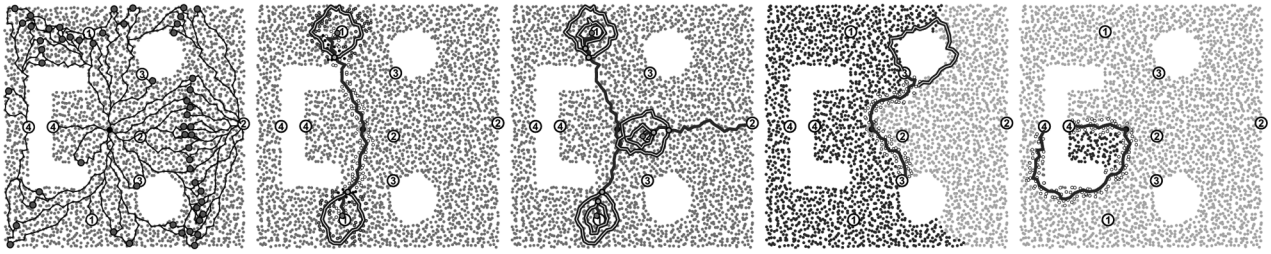


Fig. 6. Wormhole detection in discrete environments. (a) Constructing shortest path tree and cut pairs. (b) Detecting independent nonseparating loops. (c) Locating Class-I or Class-II wormholes. (d) Seeking knit nonseparating loop pairs. (e) Separating loops formed by Class-IV wormholes.

cross in odd times, thus l and l' are both nonseparating according to Lemma 4. On the other hand, since the original surface is homotopic to a plane area with holes, according to Jordan Curve Theorem [20], a loop in the original surface must separate the original surface into at least two components. Hence, both l and l' are separating, which leads to contradiction and finishes this proof. ∎

Theorem 6 shows that our detection method is accurate on Class-III and Class-IV wormholes, i.e., each pair of knit nonseparating loops captures at least one Class-III or Class-IV wormhole. We successively show by Theorems 7 and 8 that our method detects all topologically detectable wormholes on the original surface.

Theorem 7: The instant Class-IV wormhole is homotopy-equivalent to a plain bridge on previous surface, and thus is undetectable with topological method.

Proof: As we characterize in Section IV-B, an instant Class-IV wormhole adds a bridge on the same boundary. In the sense of homotopy equivalence, it is indistinguishable with a plain bridge on previous surface. Thus, a Class-IV wormhole is undetectable with topological method. ∎

Theorem 8: Given the original surface $\tau_0 = \tau(0, 0, b_0)$, and the surface $\tau(g, d, b)$ after wormhole attacks. Our method locates all d Class-I and Class-II wormholes and detects at least g Class-III or Class-IV wormholes, while the rest of wormholes are topologically undetectable.

Proof: First, according to Theorem 5, our method is able to locate all d Class-I and Class-II wormholes exactly. Second, according to Theorem 6, we can detect at least g Class-III or Class-IV wormholes by detecting g nonseparating loop pairs for genus g. Third, we consider an arbitrary order of inserting the wormholes into the network. According to Theorems 1 and 2, an increase of genus happens when and only when instant Class-III wormholes (might be Class-IV to the original surface) are inserted. While the genus is increased by g, there are $g + b - b_0$ instant Class-IV wormholes inserted. According to Theorem 7, their topological impacts on the network are indistinguishable from bridges and thus topologically undetectable. ∎

V. Wormhole Detection in Discrete Environments

We have characterized the impact of wormholes and described the principles of wormhole detection under continuous settings in Section IV. In this section, we present our approach in discrete environments. The principle of this design follows what we introduced in the continuous settings. When applied in discrete environment, however, there exist substantial technical challenges in transforming the principles into concrete protocols as follows.

1) It is nontrivial to test in discrete networks whether or not a cycled path is contractible, especially with only connectivity information among local neighborhoods.
2) Determining the crossing of two curves without any geometric information is challenging. To calculate the accurate crossing times of the two curves is even more difficult.
3) To seek the knit nonseparating loop pairs, we need to check whether a candidate loop is one-sided or two-sided. Having solely the connectivity information, to determine the two sides of a path is also difficult.

We address the above challenges in this design, which includes three components: *candidate loop selection*, *finding independent nonseparating loops*, and *seeking knit nonseparating loop pairs*. We illustrate the operations using the example shown in Fig. 6, where we have all four different types of wormholes residing in a network, denoted from 1 to 4.

A. Candidate Loop Selection

After the shortest-path tree is established, each node knows its shortest paths to the root node. The neighboring nodes exchange the information of their shortest paths. There are some pairs of nodes connected with each other, but with their least common ancestor far away. These nodes form *cut pairs* [24]. The cut pairs witness the candidate loops. The two shortest paths from the cut pair constitute a loop, and we qualify a candidate loop by setting a threshold on the length of the loop. The threshold depends on the expectation of the span of wormhole attacks, i.e., if we aim to detect all wormholes across h-hop span, we can set the threshold to h hops. Fig. 6(a) plots the detected cut pairs (big nodes) and corresponding candidate loops (thin line paths). The shortest-path tree is constructed by flooding from the big root node in the center. As shown in this example, there are variations on the candidate loops, including misreported ones. Due to the randomness and discreteness of the network deployment, it is indeed difficult to obtain the cut locus accurately under discrete settings. To tackle this problem, we perform all consecutive operations on all candidate loops instead of selecting only one loop for each cut path as in continuous principles.

B. Finding Independent Nonseparating Loops

Let l denote a candidate loop. To test whether l passes a Class-I or Class-II wormhole, we verify whether or not l is an

independent nonseparating loop. As described in Section IV, we need to find a small contractible circle that crosses l one time.

We articulate the concept of contractible circle in discrete settings. Given the communication graph G, and two positive integers k and δ. For a vertex $v \in V(G)$, let $\Gamma_k(v)$ denote the set of nodes within k-hop distance to v. $v \in \Gamma_k(v)$. Let $\Gamma_{k,\delta}(v) = \Gamma_{k+\delta}(v) - \Gamma_k(v)$. Given a vertex set $U \subseteq V(G)$, let $G(U)$ denote the vertex induced subgraph of G from U. Thus, for an arbitrary node $v \in V(G)$ and $r, \delta \in \mathbb{N}$, if $G(\Gamma_{k,\delta}(v))$ is a connected circular strip, we find a skeleton circle within $G(\Gamma_{k,\delta}(v))$. Tracing such a skeleton circle is nontrivial. We conduct a restricted flooding from an arbitrary node in the strip graph $G(\Gamma_{k,\delta}(v))$ and build a shortest-path tree, We find an arbitrary cut pair among the leaf nodes and connect them into a loop, similarly as what we do for constructing foregoing candidate loops. We record it as $C(v, r, \delta)$. Apparently, when r and δ are sufficiently small, $C(v, r, \delta)$ is contractible. Moreover, we say that $\Gamma_k(v)$ is a k-hop contractible disk at v if for any $r_0 \leq r \leq k$, there exists a skeleton circle within $G(\Gamma_{k,\delta}(v))$. A contractible disk represents a set of network nodes embedded in a geometric region without voids, and the skeleton circles on different levels of the contractible disk are all contractible circles. In our later example and simulations, we set $r_0 = 1$, $k = 3$, and $\delta = 2$.

By creating a contractible disk, we explore the existence of contractible circle $C(v, r, \delta)$ around each node v in the candidate loop l. If there exists such a circle $C(v, r, \delta)$, there must be intersection between $C(v, r, \delta)$ and l. In the discrete settings, however, with only network connectivity information, it is yet challenging to determine how many times $C(v, r, \delta)$ crosses l. The two general curves might intersect with no common nodes or even at multiple ambiguous intersection nodes. Fortunately, we can restrictively transform our case into a relatively easier one, as we only need to judge if $C(v, r, \delta)$ crosses l once or not. We let $\Gamma_1(C)$ and $\Gamma_1(l)$ denote the sets of nodes within one-hop distance to $C(v, r, \delta)$ and l, respectively. Let $I = \Gamma_1(C) \cap \Gamma_1(l)$. We check if there is only one single connected component in I or not and accordingly conclude if $C(v, r, \delta)$ crosses l only in one time. We confirm that the candidate loop l is an independent nonseparating loop if our test shows that $C(v, r, \delta)$ crosses l one time. Thus, there must be one endpoint of the wormhole is included in $C(v, r, \delta)$. Fig. 6(b) illustrates that our approach works on a candidate loop across a Class-I wormhole. The vertical single line represents the candidate loop that passes through the wormhole. The double-line paths are the detected contractible circles that cross the candidate loop one time. The circles nodes filled with white and gray are the one-hop neighborhoods of the single-line and double-line paths, respectively. The dark dot nodes show the intersection set of the two kinds of filled circle nodes. By shrinking the contractible circles, we can eventually locate the wormhole endpoints. As shown in Fig. 6(c), this approach successfully finds the contractible circles and locates the two endpoints of the Class-I wormhole and one endpoint of the Class-II wormhole. By tracing the traffic flow from one end, we can successively locate the other end of the Class-II wormhole.

C. Seeking Knit Nonseparating Loop Pairs

To detect Class-III or Class-IV wormholes, we continue to test whether a candidate loop l passes through a Class-III or Class-IV wormhole. According to the principles in continuous case, we seek the knit nonseparating loop pair containing l.

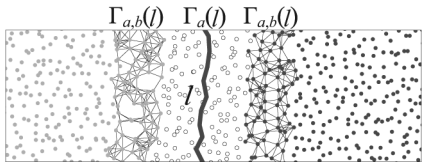


Fig. 7. Distinguishing the two sides of loop l.

The principle is simple, i.e., we conclude whether loop l is separating or nonseparating by checking whether l is one-sided or two-sided. This can be easily achieved in continuous settings by flooding two colors from l to its two sides and checking whether the two colors ultimately meet with each other. In discrete settings, however, it becomes difficult, as with only network connectivity information, we cannot distinguish the two sides of l. We cannot locally determine a node is on which side of l solely by connectivity.

We propose corresponding countermeasures to address the issue above. We first flood from loop l and construct a shortest-path tree rooted at l. Each node is thus aware of its shortest distance to l. $\Gamma_a(l)$ denotes the set of nodes within a hops to l. Indeed, as Fig. 7 shows, we let nodes in $\Gamma_a(l)$ keep silent, separating the shortest-path tree into two parts corresponding to the two sides of l. We let each node within $\Gamma_{a,b}(l)$ deliver its specific color down to successive nodes. The color is represented by its node ID or a randomly generated number. The color value is first flooded within $\Gamma_{a,b}(l)$. During flooding, the smallest color value suppresses other color values. Then, along the shortest-path tree, the dominant color value is delivered and inherited by every node. In our implementations, we set $a = 2$ and $b = 4$. After the colors spread over the network, different colors classify the nodes in the network into at least two types, as Fig. 6(d) shows. We then verify whether the nodes with different colors neighbor to each other by exchanging the color information among neighboring nodes. If there does exist such a pair, loop l is one-sided. There are two paths from the pair of nodes to loop l through the two components of different colors, and accordingly the two paths can constitute a loop l'. l and l' compose a knit nonseparating loop pair, as the pair of single-line and double-line loops found in Fig. 6(d). We then conclude that there is at least a Class-III or Class-IV wormhole on l or l'.

Fig. 6(e) displays a candidate loop formed by a Class-IV wormhole. As such a Class-IV wormhole is topologically indistinguishable from a bridge across the void hole, the loop is also tested to be separating. Our approach cannot detect such a type of wormhole, nor can any other topological approaches.

VI. Evaluation

We conduct extensive simulations under various situations to evaluate the effectiveness of our approach. By varying node placement, node density, as well as the number and type of wormholes inside the network, we evaluate the rate of successfully detected wormholes. We compare our fundamental-topology-deviations-based approach (denoted as FTD) to the packing-number-based approach (denoted as PN) proposed by Maheshwari *et al.* [9].

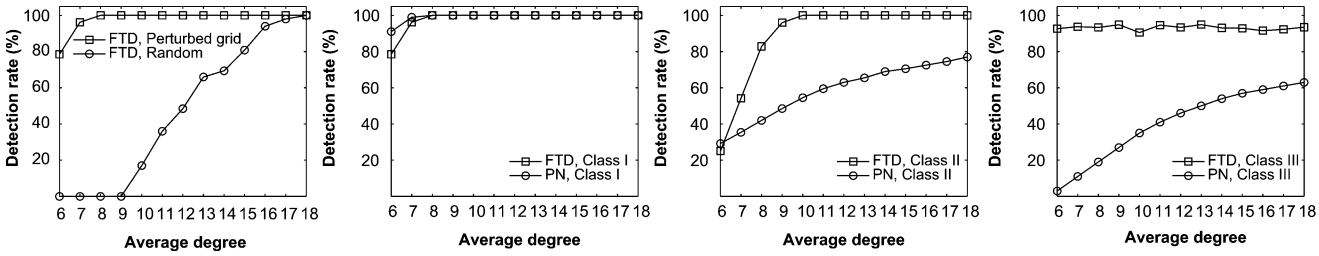


Fig. 8. Detection rates against different node degrees and types of wormholes. (a) FTD under perturbed grid and random models. (b)–(d) FTD and PN approaches detecting Class-I, Class-II, and Class-III wormholes, respectively.

A. Simulation Setup

The basic network setting is the same as the example shown in Fig. 6, i.e., a 600×600 m^2 square area with multiple holes inside. We fill the area with a network of 3200 nodes. Nodes are deployed using two models: *random placement* and *perturbed grid* [9], [24]. We use the UDG model to build the network for the convenience of comparison to the PN approach. We vary the communication radius of sensors to yield average node degrees from 6 to 18. By default, for each set of simulation, we conduct 100 runs with different node generations and report the average. We set wormholes be at least 8-hop span. Indeed, during our simulation we test our approach on various network fields of different shapes and obtain consistent results. We omit presenting the results due to the space limitation.

B. Impact of Node Placement and Density

We first test the impact of different node placements and densities on our approach. In each run, we randomly place one wormhole inside the network. Fig. 8(a) plots the wormhole detection rates of our approach under the two deployment models, where the wormhole detection rate increases as the node density increases. For the perturbed grid model, the detection rate rapidly rises up to nearly 100% when the average node degree is above 8. The random deployment provides slightly lower but still increasing detection rates. It approaches 100% when the average node degree increases to 18. Generally, the performance in random node deployment is not as satisfactory as perturbed grid due to more irregularities in the random deployment. When the node density is small (average node degree <12), it is difficult for one node to find discrete circles of sufficiently small sizes to verify the nonseparating loops (pairs) because of the poor connectivity.

C. Impact of Different Types of Wormholes

We compare our FTD approach with the PN approach. We test the detection rates of the two approaches against Class-I, Class-II, and Class-III wormholes under different node densities. We place the nodes in the perturbed grid model and randomly generate one wormhole in the network. For the packing-number-based approach, we set the forbidden parameter $f_1 = 3$, which has been shown effective for most cases in [9]. The results are displayed in Fig. 8(b)–(d). For Class-I wormholes, both our approach and the packing-number-based approach can achieve nearly 100% detection rate even under low node density. For the cases of Class-II and Class-III wormholes, the packing-number-based approach bears relatively low detection rate, while our approach rapidly approaches 100% detection rate when the node degree rises above 9. This is mainly because in the packing-number-based approach, the probability of the appearance of forbidden structures around Class-II and Class-III wormholes reduces dramatically when wormhole endpoints locate on network boundaries. Instead, our approach successfully captures the global impact of Class-II and Class-III wormholes by detecting nonseparating loops. Furthermore, an interesting behavior can be observed from Fig. 8(d). The detection rate of Class III in our approach is independent of the average node degree. This is because the partner loops in the detection of Class-III wormholes are much longer than the locally contractible cycles in the case of Class I and II. These long cycles can still form even when the average degree is relatively low.

VII. Conclusion

Wormhole attack is a severe threat to wireless ad hoc and sensor networks. Most existing countermeasures either require specialized hardware devices or have strong assumptions on the network, leading to low applicability. In this paper, we fundamentally analyze the wormhole issue by topology methodology and by observing the inevitable topology deviations introduced by wormholes. We generalize the definition of wormholes, classify the wormholes according their impacts on the network, and propose a topological approach. By detecting nonseparating loops (pairs), our approach can detect and locate various wormholes and relies solely on topological information of the network. To the best of our knowledge, we make the first attempt toward a purely topological approach to detect wormholes distributedly without any rigorous requirements and assumptions. Our approach achieves superior performance and applicability with the least limitations.

Acknowledgment

The authors are grateful for a variety of valuable comments from the anonymous reviewers.

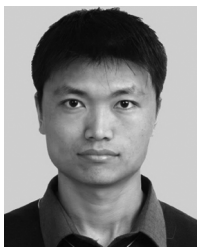
References

[1] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," presented at the SCS CNDS, San Antonio, TX, Jan. 27–31, 2002.

[2] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. IEEE ICNP*, 2002, pp. 78–87.

[3] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM*, 2003, vol. 3, pp. 1976–1986.

[4] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," presented at the NDSS, 2004.
[5] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proc. ACM WiSe*, 2004, pp. 51–60.
[6] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 6, pp. 483–503, 2006.
[7] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in *Proc. IEEE ICNP*, 2006, pp. 75–84.
[8] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Netw.*, vol. 13, pp. 27–59, 2007.
[9] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc. IEEE INFOCOM*, 2007, pp. 107–115.
[10] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Sector: Secure tracking of node encounters in multihop wireless networks," in *Proc. ACM SASN*, 2003, pp. 21–32.
[11] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: A light-weight countermeasure for the wormhole attack in multihop wireless networks," in *Proc. DSN*, 2005, pp. 612–621.
[12] I. Khalil, S. Bagchi, and N. B. Shroff, "Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks," in *Proc. IEEE SecureComm*, 2006, pp. 1–12.
[13] N. Song, L. Qian, and X. Li, "Wormhole attack detection in wireless ad hoc networks: A statistical analysis approach," in *Proc. IEEE IPDPS*, 2005.
[14] L. Buttyan, L. Dora, and I. Vajda, "Statistical wormhole detection in sensor networks," in *Proc. IEEE ESAS*, 2005, pp. 128–141.
[15] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 4, pp. 791–802, Aug. 2008.
[16] Ö. B. Akan and I. F. Akyildiz, "Event-to-sink reliable transport in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 5, pp. 1003–1016, Oct. 2005.
[17] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 247–260, Feb. 2006.
[18] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A secure sensor network communication architecture," in *Proc. ACM/IEEE IPSN*, 2007, pp. 479–488.
[19] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. ACM SenSys*, 2004, pp. 162–175.
[20] A. Hatcher, *Algebraic Topology*. Cambridge, U.K.: Cambridge Univ. Press, 2002.
[21] K. Whittlesey, "Greedy optimal homotopy and homology generators," in *Proc. ACM-SIAM SODA*, 2005, pp. 1038–1046.
[22] J. Erickson and S. Har-Peled, "Optimally cutting a surface into a disk," in *Proc. ACM SCG*, 2002, pp. 244–253.
[23] M. J. Pelsmajer, M. Schaefer, and D. Stefankovic, "Removing even crossings, continued," in *DePaul CTI 06-016*, Aug. 28, 2006, pp. 1–14.
[24] Y. Wang, J. Gao, and J. S. Mitchell, "Boundary recognition in sensor networks by topological methods," in *Proc. ACM MobiCom*, 2006, pp. 122–133.

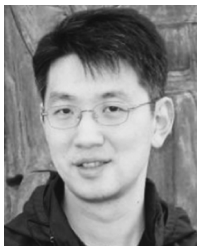


Dezun Dong (S'09–M'10) received the B.S., M.S., and Ph.D. degrees in computer science at National University of Defense Technology (NUDT), Changsha, China, in 2002, 2004, and 2010, respectively.

He was a Visiting Scholar with the Computer Science and Engineering Department, Hong Kong University of Science and Technology, Hong Kong, from November 2008 to May 2010. He is currently an Assistant Professor with the School of Computer, NUDT. His research interests are wireless networks, distributed computing, and high-performance computer systems.

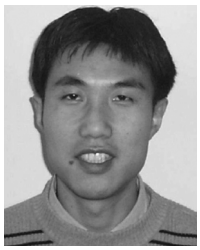
Mo Li (M'06) received the B.S. degree in computer science and technology from Tsinghua University, Beijing, China, in 2004, and the Ph.D. degree in computer science and engineering from Hong Kong University of Science and Technology, Hong Kong, in 2009.

He is a Nanyang Assistant Professor with the Computer Science Division, School of Computer Engineering, Nanyang Technological University, Singapore. His research interests include distributed systems, wireless sensor networks, pervasive computing and RFID, and wireless and mobile systems.



Yunhao Liu (M'02–SM'06) received the B.S. degree in automation from Tsinghua University, Beijing, China, in 1995, and the M.S. and Ph.D. degrees in computer science and engineering from Michigan State University, East Lansing, in 2003 and 2004, respectively.

He is a Professor with the Tsinghua National Lab for Information Science and Technology, School of Software, and the Director of the MOE Key Lab for Information Security, Tsinghua University. He is also a faculty member with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong.



Xiang-Yang Li (SM'08) received the B.S. degree from Tsinghua University, Beijing, China, in 1995, and the M.S. and Ph.D. degrees from the University of Illinois at Urbana–Champaign in 2000 and 2001, respectively, all in computer science.

Currently, he is an Associate Professor with the Department of Computer Science, Illinois Institute of Technology, Chicago. His research interests span wireless ad hoc networks, computational geometry, game theory, and cryptography and network security.

Xiangke Liao received the B.S. degree in computer science from Tsinghua University, Beijing, China, in 1985, and the M.S. degrees in computer science from the National University of Defense Technology (NUDT), Changsha, China, in 1988.

He is now a Professor and the Dean of the School of Computer, NUDT. His research interests include parallel and distributed computing, high-performance computer systems, operating system, and networked embedded system.