

Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks

Dezun Dong^{*†}, Mo Li[†], Yunhao Liu[†], Xiang-Yang Li[‡], and Xiangke Liao^{*}

^{*}School of Computer, National University of Defense Technology, Changsha, China

[†]Dept. of Computer Science and Engineering, Hong Kong University of Science and Technology

[‡]Dept. of Computer Science, Illinois Institute of Technology, Chicago, IL, USA

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 work, 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 rigorously prove the correctness of this design in continuous geometric domains and extend it into discrete domains. We evaluate its performance through extensive simulations.

I. INTRODUCTION

Wireless ad hoc and sensor networks are emerging as promising techniques for ubiquitous data exchange and information sharing. A particularly severe attack against wireless ad hoc and sensor networks is wormhole attack, which has been independently introduced in previous works [14] [9] [17]. In wormhole attacks, the attackers tunnel the packets between distant locations in the network through a high-speed out-of-band channel. The wormhole tunnel gives two distant nodes the illusion that they are close to each other. By building these wormhole tunnels, the attackers attract a large amount of network traffic and thus, are able to launch a variety of attacks, e.g., the attackers can selectively drop specified packets, forward packets out of order, modify packets, etc. More importantly, by collecting packets for analyzing traffic or compromising cryptographies, adversaries are able to use the wormhole attack as a stepping stone for many other more aggressive and severe attacks, such as network hijacking, man-in-the-middle attacks, and cipher breaking, significantly imperiling routing, localization, topology control, as well as many other network protocols [9]. Since the wormhole attack can be launched without compromising any legitimate node or cryptographic mechanisms [9], most generic security mechanisms are vulnerable to such attacks.

The wormhole attack problem has received considerable attentions recently. 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 wormhole. 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 [9] [20], directional antennas [8], or special radio transceiver modules [2], which introduce significant amounts of extra hardware costs for the systems. Other types of approaches are based on strict assumptions, such as global tight clock synchronization [9], special guard nodes [12], attack-free environments [10], or unit disk communication models [13]. These rigorous requirements and assumptions largely restrict their applicability in networks composed of a large number of low-cost resource-constrained nodes.

To fully address wormhole attack in ad hoc and sensor network, 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 (possibly with irregular boundaries, inner obstacles, or even on a non-2D plain) 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 exceptions. Our approach solely explores the topology of the network connectivity. 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. The detection algorithm is carried out in a distributed manner across the network to avoid dependence on a small portion of the network, which could become the target of the adversaries.

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. In Section IV, we characterize the wormhole in topologies and describe theoretical principles of a fundamental detection method. Section V extends this design into discrete networks and shows the details of the detection protocol. We evaluate this design through extensive simulations in Section VI, and conclude the 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. [9] 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. [20] instead verify the end-to-end distance bounds between the source and the destination nodes. Zhang et al. [22] propose location-based neighborhood authentication scheme to locate the wormholes. Such approaches require the pre-knowledge of network locations to capture the distance mismatch.

Some approaches observe the symptom of time mismatch in packet forwarding. Hu et al. [9] introduce temporal packet leash, which assumes tight global clock synchronization and detects wormholes from exceptions in packet transmission latency. Capkun et al. [2] 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. TrueLink proposed by Eriksson et al. [5] is another RTT based approach. It relies on the exchange of vast verifiable nonces between neighboring nodes. They modify the standard IEEE 802.11 protocols for the implementation. It remains unclear how effective such an approach is for the resource constraint ad hoc or sensor network hardware.

Some approaches observe the symptom of neighborhood mismatch that leads to physical infeasibility. Hu et al. [8] adopt directional antennas and find infeasible communicating links by utilizing the directionality of antenna communication. Khalil et al. [10] 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 channel by overhearing the infeasible transmissions among non-neighboring nodes. They further propose MobiWorp [11] to complement LiteWorp with the assistance of some location-aware mobile node.

Some approaches observe the symptom of graph mismatch under special assumptions of network graph models. Poovendran et al. [12] [16] present a graph based framework to tackle wormholes. Their approach assumes the existence of guard nodes with extraordinary communication range. The direct communication links between guard nodes and regular nodes implicitly form a geometric graph and the wormholes will break the constraints. Wang et al. [19] graphically visualize the presence of wormholes. They reconstruct the layout of the networks by multi-dimensional scaling (MDS). Through the distance measurements between neighboring nodes, a central controller calculates the network layout and captures the wrap introduced by wormholes. Recently, authors in [13] propose a completely localized approach to detect wormholes with only network connectivity. By exploiting the forbidden packing number in the Unit Disk Graph (UDG) embedding of network graphs, the approach is able to detect wormholes with high accuracy. As a clear and elegant approach, however, it has its own limitations due to the assumption of UDG graph model and its basis on the symptom of packing number. It may fail when a wormhole does not cause an increase of packing number. It is thus inaccurate under non-UDG graphs.

Some approaches observe the symptom of traffic flow mismatch based on statistic analysis on the network traffic. Song et al. [18] 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. [1] 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 pre-statistics of normal networks.

To sum up, existing approaches heavily rely on specialized hardware or rigorous assumptions to capture the wormhole symptoms. Indeed, there are still no perfect symptoms found to establish an all-round method in the resource-limited ad hoc and sensor networks. Our design, based on topological observation, is orthogonal to existing approaches and takes a step towards relaxing these assumptions and expanding the applicability of methods.

III. PROBLEM FORMULATION

Poovendran et al. gave a formal definition of the wormhole problem based on the UDG communication graph model in Euclidean space [16]. According to their definition, a communication link is a wormhole link if the distance between its two endpoints exceeds the regular communication range. This concise definition, however, also has its own limitations. First, the definition is given under the constraints of the UDG communication graph model, which has been proven far from practical in many analytical and experimental works. Second, the distance-based definition in Euclidean space naturally binds the wormhole features with external geometric environments, and thus neglects the inherent topological impacts

introduced by wormholes. We hereby present a more general and fundamental definition of the wormhole attack based only on network topologies and aim to present the inherent characteristics of wormholes.

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 Pooven-dran 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. We then present our definition on generalized wormhole detection method.

Definition 2: (Generalized Wormhole Detection Methods) Let $\mathcal{G}_L \subseteq \mathcal{G}$ denote the set of legitimate network communication graphs, where \mathcal{G} is the set of arbitrary communication graphs. Let \mathcal{K} denote the pre-knowledge on legitimate network communication graphs. Let \mathcal{P} denote the set of network properties, including graph or topological invariants. $\mathcal{M}_K : \mathcal{G} \rightarrow \mathcal{P}$ is a mapping from the set of communication graphs to the set of network properties. If for any $G \in \mathcal{G}_L$, $\mathcal{M}_K(G) \subseteq \mathcal{M}_K(\mathcal{G}_L)$, \mathcal{M}_K provides a detection method, which does not cause false positive results. If for any graph $G \notin \mathcal{G}_L$, $\mathcal{M}_K(G) \not\subseteq \mathcal{M}_K(\mathcal{G}_L)$, \mathcal{M}_K is a detection method without false negative. \mathcal{M}_K is a perfect method if it produces neither false negative nor false positive results.

Essentially, Definition 2 covers all possible methods that rely on network topologies for detecting wormholes. Different specific methods differ on assuming what pre-knowledge on the legitimate network and exploring what properties of the network topologies. For example, we explain this by an instance of wormhole detection methods which has been recently introduced by Maheshwari et al. [13]. Their method assumes a pre-knowledge \mathcal{K} that the legitimate network communication graph is UDG, and mainly relies on the property $P \in \mathcal{P}$ that the lune packing number in an UDG embedding of the legitimate network communication graph is 2.

IV. CHARACTERIZING WORMHOLES

In this section, we model and characterize wormhole attacks on network topologies, and then propose the detection approach accordingly. Aiming at a distributed algorithm based on minimum assumptions on the pre-knowledge of a network, we intend to detect wormholes by solely depending

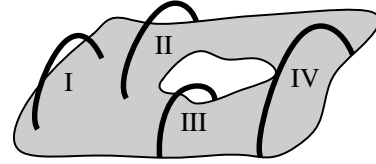


Fig. 1: Four different types of wormholes on the surface.

on local cooperation and estimations. Nevertheless, the topological impact of wormholes is global, so how to characterize the global properties of wormholes from local information becomes a major challenge.

We address the above problem through algebraic topology, by using homology and homotopy in general topological space. We introduce concepts, develop principles and present related theorems in continuous domain. We first introduce topological preliminaries. We then characterize the topological features of wormholes and classify the wormholes. Finally, we present the principles for the wormhole detection and prove theoretical guarantees. We extend our discussion to practical discrete networks in the next section.

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, see the books by Hatcher [7].

Given a topological space T , a *path* is a continuous function $p : [0, 1] \rightarrow T$; a path whose endpoints coincide is called a *loop*. A *homotopy* between two paths p and q with the same endpoints is a continuous function $h : [0, 1][0, 1] \rightarrow T$, such that $h(0, t) = p(t)$ and $h(1, t) = q(t)$ for all t , and $h(s, 0) = p(0) = q(0)$ and $h(s, 1) = p(1) = q(1)$ for all s . Two paths are *homotopic* if there is a homotopy from one to the other. A loop is *contractible* if it is homotopic to a point.

In our work, we consider network deployment region as connected, compact and orientable (two-sided) 2-manifold *surfaces* that are topological Hausdorff spaces, 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. When topological space T is a given surface S , a *curve* is a path and a *closed curve* is a loop. A *simple closed curve* is an injective closed curve that does not intersect itself. Two curves with the same endpoints on S 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 *non-contractible*. A closed curve is *non-separating* if the surface keeps connected after its removal. A closed curve is *separating* if it splits the surface into two 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 is actually an equivalence relation on the set of closed curves on S 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.

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. Figure 1 shows the four types of wormholes. For Class I wormhole, both of its two endpoints locate inside the surface. Class II wormhole has one endpoint inside the surface and the other on the boundary of the surface. Class III wormhole has its endpoints on two different boundaries. 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.

1) Single wormhole impact:

We first consider the impact of a single wormhole. We then analyze the impact of the combination of multiple wormholes.

a) *Class I and II wormholes*. Figure 2 shows an example of how a spherical surface X is affected by a wormhole link AB , which represents a Class I or II wormhole. Figure 2 (a) shows the new topology *quotient space* $X \setminus AB$ [7], with link AB glued on the spherical surface X . Figure 2 (b) shows a homotopy equivalent topology with (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 Figure 2 (c). By contracting a longitudinal cycle around the torus, Y collapses into $X \setminus AB$. Clearly, such a collapse is not a homotopy equivalence from Y to $X \setminus AB$. In this sense, we say that $X \setminus AB$ contains degenerated genus 1. Strictly speaking, the new topology space after the injection of Class I or 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 as a surface with singularities.

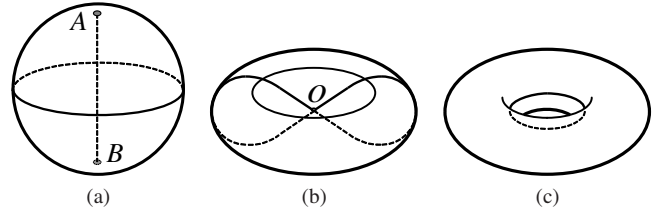


Fig. 2: (a) Link AB glued on a spherical surface X ; (b) Link AB is contracted to a single point O ; (c) Torus Y , which may collapse into $X \setminus AB$ by contracting a longitudinal cycle into one point.

b) *Class III wormholes*. When the surface is of multiple boundaries (the network containing physical holes), Class III wormhole might appear as shown in Figure 3 (a). The topology space of Figure 3 (a) is homotopy equivalent to that in Figure 3 (b), which contracts the wormhole link into a point. We focus on the two non-contractible cycles α and β in Figure 3 (b). Cycle α goes through the wormhole, and cycle β wraps the inner boundary. Figure 3 (b) can be seen as the deformation retract of Figure 3 (c), where the cycles α and β in Figure 3 (c) correspond to α and β in Figure 3 (b) respectively. Indeed, Figure 3 (a-c) are 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 Class III wormhole. The twisted cycle α and cycle β are actually symmetrical to each other in the sense of topology. Imaging that if we overturn the surface in Figure 3 (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 Figure 3 (b) through only topologies.

c) *Class IV wormholes*. A Class IV wormhole connects two points on the same boundary. Thus 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.

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

2) Combination of multiple wormholes:

When two or more wormholes exist on the surface, Class I or 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 Figure 3 (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, Figure 3 (d) is homotopy equivalent to Figure 3 (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

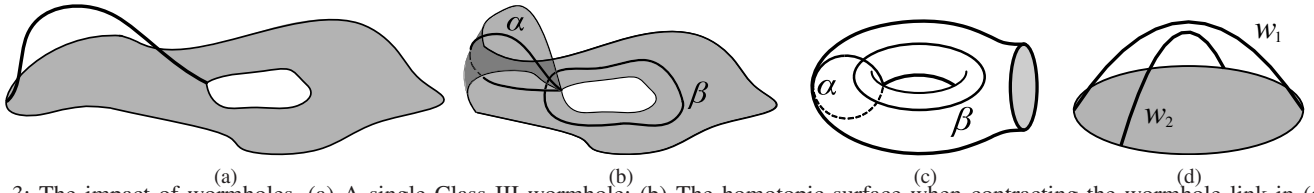


Fig. 3: The impact of wormholes. (a) A single Class III wormhole; (b) The homotopic surface when contracting the wormhole link in (a); (c) The homotopic surface to (a) and (b); (d) Two Class IV wormholes crossing each other.

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 the instant surface when it is glued. Class I and II wormholes will not be affected by previous injected wormholes, while Class III and 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 non-negative 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 II wormholes and $2(g - g_0) + b - b_0$ Class III or IV wormholes.

According to our per-knowledge 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. In real implementation, the algorithm does not depend on centralization throughout the network. A node makes decisions solely based on its local information.

The proposed algorithm aims to trace wormholes through detecting the genus and degenerated genus. The main idea of the algorithm is to find the non-separating cycles associated with wormholes. Figure 4 (a) shows an example of a surface with wormholes where the two circular lines indicate two potential non-separating cycles.

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 [4], as shown in Figure 4 (b). 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* [4], 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 cut locus which has at least three shortest paths to the root is called a *branch vertex* of the cut locus, like point v in Figure 4 (b). The branch vertices separate the cut locus into *cut paths*, like path p_1 , p_2 and p_3 in Figure 4 (b). Each cut path has two endpoints. The endpoint of a cut path can be a branch vertex or not. We call the endpoint *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 *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 [4]. 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 non-homotopic shortest paths from a to the root. By concatenating the two non-homotopic paths, we obtain a loop l_a and it is clear that loop l_a is non-contractible. 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 [4]. 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*. Figure 4 (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 Figure 4 (b) respectively. Following Lemma 4.2 in [3], 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 II wormholes:

To begin with, for checking whether or not the loop passes through a degenerated genus (Class I or 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 Figure 4 (d), the bold line denotes the candidate loop l , which passes through a

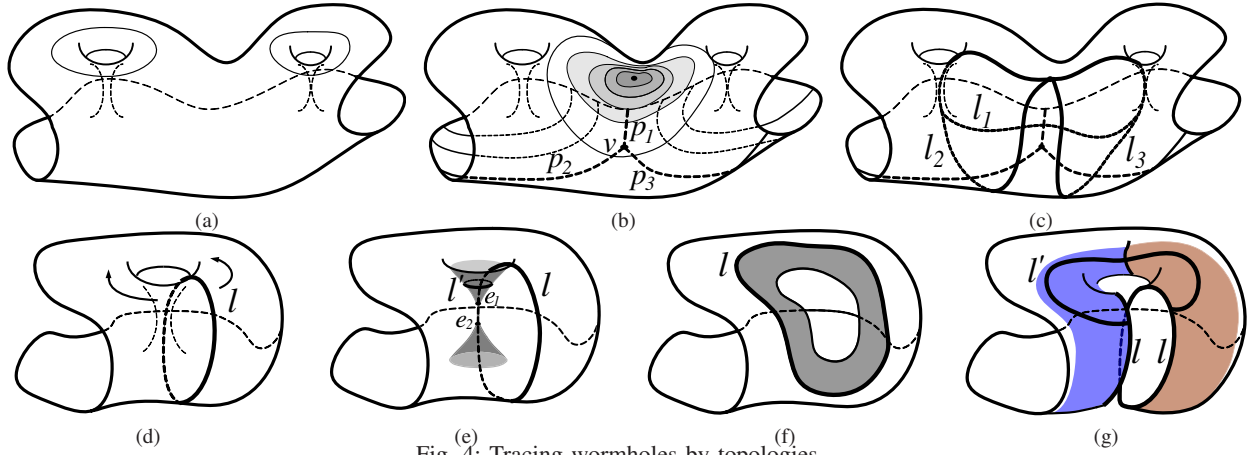


Fig. 4: Tracing wormholes by topologies.

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 [7]), l can be marked as a loop through Class I or II wormhole. We call l an *independent non-separating 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 Figure 4 (d). By this means, we can detect the endpoints of all Class I and II wormholes.

3) Detecting Class III or IV wormholes:

The case of Class III and IV wormhole 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 non-separating loop. There is an essential difference between the two types of loops. The separating loop is two-sided but the non-separating loop is one-sided. Figure 4 (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., red and blue to its two sides, the two colors never meet. The loop shown in Figure 4 (f), however, is a non-separating loop formed by genus. If we flood red and blue to its two sides, as shown in Figure 4 (g), the two colors ultimately meet with each other because the loop is one-sided. By detecting the non-separating loop l , we detect the genus introduced by Class III or Class IV wormholes. Let t be a point on the cut between red and blue areas. Let $s \in l$ be an arbitrary point on l . There is a pair of non-homotopic paths from s to t , one across the red area and the other one across the blue area. The two paths form a loop, which we denote in Figure 4 (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 non-separating loops. We call l a *dependent non-separating loop* and l' the *partner loop* of l . Further, we call the two non-separating loops that cross each other *knit non-separating loop pair*. We can conclude that there must be at least one Class III or IV wormhole in the knit non-separating loop pair. Yet as we mention in Figure 3 (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 non-separating loop, or dependent non-separating loop. We detect and locate Class I and II wormholes from independent non-separating loops. We detect Class III and IV wormholes from dependent non-separating 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 [4]. 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 II wormholes. We first present Lemma 4, which reveals the parity property of the non-separating loops.

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

Proof: Following Lemma 2.1 in [15], if c is separating, $S - c$ has two components S_1 and S_2 , each with c as its boundary. If we trace the curve c' , it must switch between S_1 and S_2 each time it crosses c , and never otherwise. Hence there must be an even number of switches, contradicting the fact that c and c' cross oddly. ■

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

Proof: Let w be an arbitrary Class I or II wormhole. According to Theorem 3, there exists a loop $l_w \in L$ which passes through w . Since w is a Class I or 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 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 non-separating. l' is both non-separating 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 II wormholes. ■

Theorem 6: Let l and l' be a pair of knit non-separating loops. There is at least one Class III or 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 non-separating loop pair, l and l' cross in odd times, thus l and l' are both non-separating 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 [7], 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 IV wormholes, i.e., each pair of knit non-separating loops captures at least one Class III or IV wormhole. We successively show by Theorem 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 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 II wormholes and detects at least g Class III or 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 II wormholes exactly. Second, according to Theorem 6, we can detect at least g Class III or IV wormholes by detecting g non-separating loop pairs for genus g . Third, we consider an arbitrary order of inserting

the wormholes into the network. According to Theorem 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 the previous section. In a real multi-hop network, however, nodes are deployed discretely on the field. In this section, we present our approach in discrete environments. First, we construct a shortest path tree from an arbitrarily selected root node, so that each node obtains shortest paths to the root. We accordingly select the candidate loops from the cut pairs on the shortest path tree. Second, we detect and locate Class I or II wormholes by testing whether a candidate loop is an independent non-separating loop. Specifically, we check whether there exists a contractible cycle that crosses the loop one time. Third, we check the existence of Class III or IV wormholes by seeking the knit non-separating loop pairs. All operations are carried out in a distributed manner in the discrete network. 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 non-trivial 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 non-separating loop pairs, we need to check whether a non-separating 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 above challenges in this design, which includes three components: *Candidate Loop selection*, *Finding Independent Non-Separating Loops*, and *Seeking Knit Non-Separating Loop Pairs*. We illustrate the operations using the example shown in Figure 5, 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* [21]. The cut pairs witness the candidate loops. The two

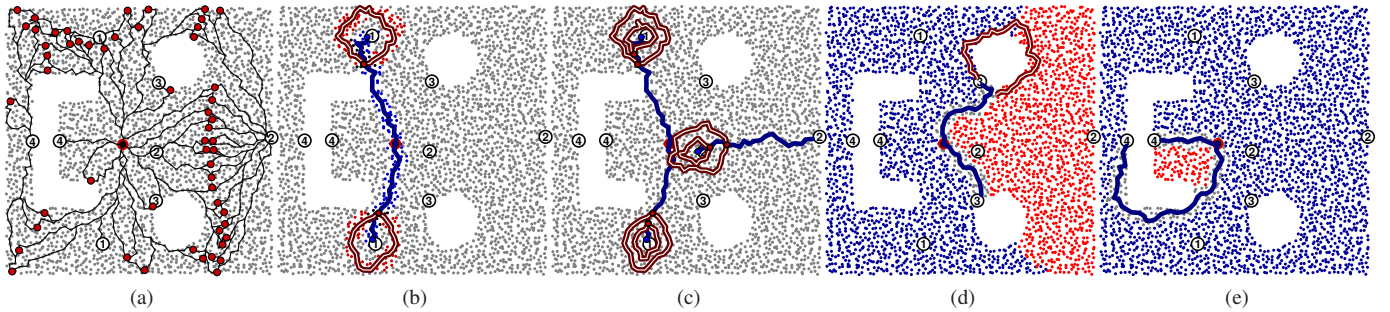


Fig. 5: Wormhole detection in discrete environments.

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.

Figure 5 (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. Such operations might introduce extra network cost. In practice, we can filter most of redundant candidate loops simply by checking their neighboring relationship, which leads to significant savings on the overhead.

B. Finding Independent Non-Separating Loops

Let l denote a candidate loop. To test whether l passes a Class I or II wormhole, we verify whether or not l is an independent non-separating loop. As described in previous section, 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 non-trivial. 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. Similar problems are also considered in [6]. 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 once one time. We confirm that the candidate loop l is an independent non-separating loop if our test shows that $C(v, r, \delta)$ crosses l one time. Thus there must be one endpoint of the wormhole included in $C(v, r, \delta)$. Figure 5 (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 red double-line paths are the detected contractible circles that cross the candidate loop one time. The deep blue and red nodes near the lines are the one-hop neighborhoods of the lines, respectively. The black nodes show the intersection of blue and red node sets. By shrinking the contractible circles, we can eventually locate the wormhole endpoints. As shown in Figure 5 (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 Non-Separating Loop Pairs

To detect Class III or IV wormholes, we continue to test whether a candidate loop l passes through a Class III or IV

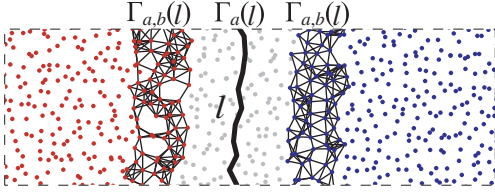


Fig. 6: Distinguishing the two sides of loop l .

wormhole. According to the principles in continuous case, we seek the knit non-separating loop pair containing l .

The principle is simple, i.e., we conclude whether loop l is separating or non-separating by checking whether l is one-sided or two-sided. This can be easily achieved in continuous settings by flooding red and blue 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 by solely 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 hop to l . Indeed, as Figure 6 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 $\Gamma_{a,b}(l)$ delivers 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 Figure 5 (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 non-separating loop pair, as the pair of blue single-line and double-line loops found in Figure 5 (d). We then conclude that there is at least a Class III or Class IV wormhole on l or l' .

Figure 5 (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 wormholes, neither any other topological approaches.

VI. EVALUATION

We conduct extensive simulations under various situations to evaluate the effectiveness of our approach. By varying

node density, 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) with the packing number based approach (denoted as PN) proposed by Maheshwari et al. [13], which is to the best of our knowledge the only distributed method using solely node connectivity to detect wormholes.

A. Simulation Setup

The basic network setting is the same as the example shown in Figure 5, i.e., a 600m by 600m square area with multiple holes inside. We fill the area with a network of 3200 nodes. In our simulations, nodes are deployed using the model of *perturbed grid*. The perturbed grid model deploys nodes on a grid and then perturbs each node with a random shift. This model has been adopted [21] to approximate manual deployments of nodes, corresponding more closely to planned organizations of a wireless network, e.g., organizing nodes in an indoor environment. It uniformly fills sensors into the field.

Although our detection approach does not enforce the compliance to specific communication models for the network, for the convenience of comparison, we assume UDG model to build the network, which establishes the basis for the correct operation in PN approach. We vary the communication radius of sensors from 17 meters to 25 meters, yielding average node degrees from 8 to 18. 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 Density and Different Types of Wormholes

We test the impact of different node densities on our approach, and compare our FTD approach with the PN approach. We vary the density of nodes so that the average degree of each node is increased from 8 to 18. For each set of simulation, we conduct 100 runs with different node generations and report the average. In each run, we randomly place a wormhole inside the network with at least 8 hops span. We test the detection rates of the two approaches against Class I, II and III wormholes under different node densities. We randomly generate each type of wormholes with at least 8 hops span. For the packing number based approach, we set the forbidden parameter $f_1 = 3$, which has been shown effective for most cases in [13].

The results are displayed in Figure 7 (a-c). 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 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 packing number based approach, the probability of the appearance of forbidden structures around Class II and III wormholes reduces dramatically when

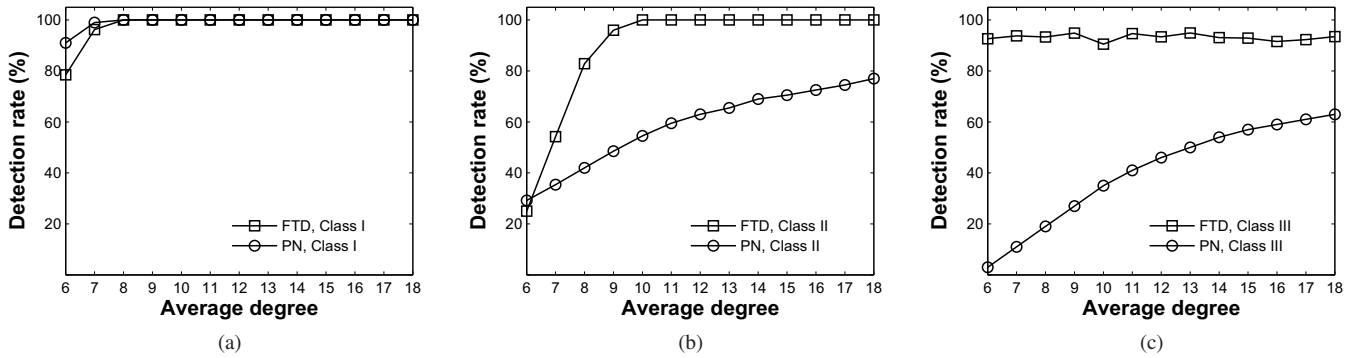


Fig. 7: Detection rates against different node degrees and types of wormholes.

wormhole endpoints locate on network boundaries. Instead, our approach successfully captures the global impact of Class II and III wormholes by detecting non-separating loops (pairs). Further, an interesting behavior can be observed from Figure 7 (c). The detection rate of Class III in our approach is independent of the average node degree. This is due to that the partner loops in the detection of Class III wormholes is 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. CONCLUSIONS

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 work, 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 non-separating 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 towards 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.

VIII. ACKNOWLEDGMENTS

The authors are grateful for a variety of valuable comments from the anonymous reviewers. This work is supported in part by the NSFC/RGC Joint Research Scheme N_HKUST 602/08, the National Basic Research Program of China (973 Program) under grant No. 2006CB303000, the National High Technology Research and Development Program of China (863 Program) under grants No. 2002AA1Z2101, No. 2007AA01Z177 and No. 2007AA01Z180, NSFC under grants No. 60621003 and No. 90718040.

REFERENCES

- [1] L. Buttyan, L. Dora, and I. Vajda, "Statistical wormhole detection in sensor networks," in *Proc. of IEEE ESAS*, 2005.
- [2] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Sector: Secure tracking of node encounters in multi-hop wireless networks," in *Proc. of ACM SASN*, 2003.
- [3] J. Erickson and S. Har-Peled, "Optimally cutting a surface into a disk," in *Proc. of ACM SoCG*, 2002.
- [4] J. Erickson and K. Whittlesey, "Greedy optimal homotopy and homology generators," in *Proc. of ACM-SIAM SODA*, 2005.
- [5] J. Erickson, S. V. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in *Proc. of IEEE ICNP*, 2006.
- [6] R. Ghrist, D. Lipsky, S. Poduri, and G. Sukhatme, "Surrounding nodes in coordinate-free networks," in *Proc. of Workshop in Algorithmic Foundations of Robotics*, 2006.
- [7] A. Hatcher, *Algebraic Topology*. Cambridge University Press, 2002.
- [8] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. of NDSS*, 2004.
- [9] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. of IEEE INFOCOM*, 2003.
- [10] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: A light-weight countermeasure for the wormhole attack in multihop wireless networks," in *Proc. of DSN*, 2005.
- [11] —, "Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks," in *Proc. of IEEE SecureComm*, 2006.
- [12] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach," in *Proc. of IEEE WCNC*, 2005.
- [13] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proc. of IEEE INFOCOM*, 2007.
- [14] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. of SCS CNDS*, 2005.
- [15] M. J. Pelsmajer, M. Schaefer, and D. Stefankovic, "Removing even crossings, continued," in *DePaul CTI 06-016*, August 28 2006.
- [16] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," vol. 13, 2007, pp. 27–59.
- [17] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proc. of IEEE ICNP*, 2002.
- [18] N. Song, L. Qian, and X. Li, "Wormhole attack detection in wireless ad hoc networks: a statistical analysis approach," in *Proc. of IEEE IPDPS*, 2005.
- [19] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proc. of ACM WiSe*, 2004.
- [20] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," vol. 6, 2006, pp. 483–503.
- [21] Y. Wang, J. Gao, and J. S. Mitchell, "Boundary recognition in sensor networks by topological methods," in *Proc. of ACM MobiCom*, 2006.
- [22] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," vol. 24, 2006, pp. 247–260.