Computer Networks 150 (2019) 190–200

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures

Sen Bai[a], Yunhao Liu[a,*], Zhenhua Li[a], Xin Bai[b]

[a] School of Software, Tsinghua University 30 Shuangqing RD, Beijing, 100084, China
[b] Huawei Technologies Co. Ltd., No. 410, Jianghong Street, Hangzhou China

ARTICLE INFO

Article history:
Received 16 May 2018
Revised 11 November 2018
Accepted 8 January 2019
Available online 12 January 2019

ABSTRACT

A wormhole in wireless ad hoc networks is a physically low-latency link that connects two topologically distant nodes. Thereby, an adversary can launch the wormhole attack by tunnelling recorded packets from one node to the other and retransmitting them in the network. Since the wormhole attack is independent of MAC layer protocols and immune to cryptographic techniques, it has been one of the most dangerous security threats to wireless ad hoc networks. At present, efficient algorithms have been applied to 2D networks to detect wormhole attacks by seeking for forbidden substructures. However, when we employ their defined forbidden substructures to detect wormhole attacks in 3D networks (which are more pervasive in reality), we encounter severe obstacles. Through an in-depth examination, we discover the existence of efficient 3D forbidden substructures by introducing *maximum independent sets* (MaxIS) into the network. Essentially different from 2D forbidden substructures, 3D forbidden substructures can hardly be intuitively perceived. Driven by above understandings, we design a MaxIS-based wormhole detection algorithm for 3D networks using only connectivity information. Furthermore, we conduct thorough theoretical analyses and illustrate that our algorithm is able to detect almost 100% wormhole attacks even in a wireless network with very poor connectivity.

1. Introduction

A wormhole in wireless ad hoc networks is a physically low-latency link that connects two topologically distant nodes, as exemplified in Fig. 1. By exploiting the specialty of wormhole, wormhole attack [1–11] has become one of the most dangerous security threats to wireless ad hoc networks. In a wormhole attack, an attacker introduces two transceivers into a wireless network and connects them with a low-latency link. Signals captured by one transceiver are tunneled through the wormhole link to the other remotely located transceiver and replayed. Once the wormhole link is established, the wireless nodes near one wormhole transceiver will be recognized as neighbors of the wireless nodes near the other wormhole transceiver. Therefore, in multi-hop wireless networks, a wormhole can attract a large amount of network traffic.

As shown in Fig. 1, the hostile put two transceivers respectively at A and B. Then the attacker tunnels the packets between A and B by a high capacity wormhole link. The signals captured by one end of the link are repeated at the other end. W_0 is neighborhood of A and W_1 is neighborhood of B. Any transmission generated by a node in W_0 will also be heard by any node in W_1. That is, a, b are both recognized as neighbors of c, d, e and vice versa. If A and B are placed at a distance far enough, nodes in W_0 and W_1 take a one-hop path via the wormhole instead of a multi-hop path and the wormhole link can attract a lot of routes.

After the attacker attracts a large amount of network traffic through the wormhole, the attacker can record the traffic for later analysis or manipulate network traffic. For example, the attacker can selectively drop or modify data packets. By turning off the wormhole link periodically, the attacker can suddenly create and destroy a large number of shortest paths in the network and significantly imperils most network routing protocols. Using wormholes an attacker can also break any protocol that directly or indirectly relies on geographic proximity. Since the network topology is changed, wormholes also affect connectivity-based localization algorithms. A wormhole attack is independent of MAC layer protocols and immune to cryptographic techniques. The wormhole can be launched at bit level or at the physical layer. Thus, wormholes are hard to detect and wormhole attacks have posed a severe threat to wireless ad hoc and sensor networks.

In the literature many countermeasures have been proposed to detect wormhole attacks in wireless ad hoc networks. These exist-

[*] Corresponding author.
E-mail addresses: baisenbx@126.com (S. Bai), yunhaoliu@gmail.com (Y. Liu), lizhenhua1983@gmail.com (Z. Li), baixinbs@163.com (X. Bai).

https://doi.org/10.1016/j.comnet.2019.01.008
1389-1286/© 2019 Published by Elsevier B.V.

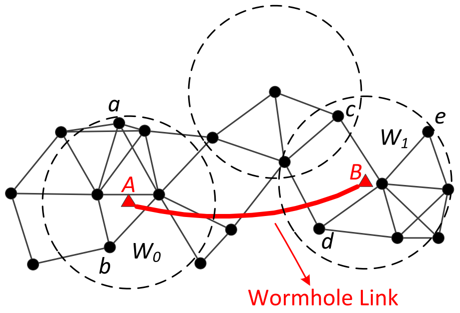


Fig. 1. An example of a wormhole [2]. *A* and *B* denote two wormhole nodes connected through a wormhole link. As a result of the attack, nodes in area W_0 are recognized as neighbors of nodes in W_1 and vice versa.

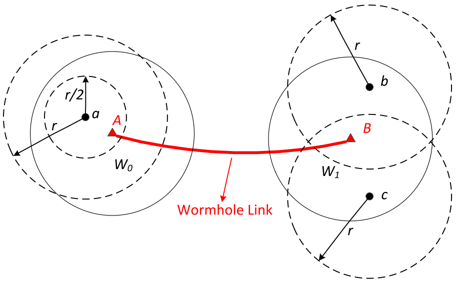


Fig. 2. Forbidden substructure based wormhole detection in delay tolerant networks [12].

ing methods have their respective limitations. Some of these methods depend on specialized hardware devices. For example, some approaches employ additional hardware devices such as directional antennas [11], GPS [8], or special radio transceiver modules. One of these types of approaches in [8] is based on ideal assumptions such as global tight clock synchronization. There are other methods using special guarding nodes [4,5,7] with known locations, higher transmit power and different antenna characteristics are limited in applicability. Some other methods using neighborhood discovery [3,9] assume that the network is free of wormhole to start with. Recently proposed wormhole detection algorithms focus on wireless network coding system [1], delay tolerant networks [12]. In another work the wormhole attack on a network control system is studied and a passivity-based control-theoretic framework for modeling and mitigating the wormhole attack is presented. Several topology-based wormhole detection approaches have been proposed [1,6,10]. The approach in [10] uses local topological changes around the neighborhood of wormhole nodes to detect wormhole links but, can hardly achieve high detection rate for networks with low node density and poor connectivity. Local connectivity test in [6] is not limited to various constraints but legal network structure such as a bridge might also be identified as a wormhole link in their definition.

Detecting wormhole attacks by network topology is a feasible solution because it does not rely on additional hardware and only connectivity information is required. In [2] a localized algorithm is proposed to detect wormhole attacks by seeking forbidden substructures. The basic idea is that 2 non-neighboring nodes have at most 2 independent common neighbors. This simple observation brings sound performance on wormhole detection but, 3D forbidden substructures can hardly be intuitively perceived and the approach has long been thought to be limited to 2D ad hoc networks. To this end, in this paper we strive towards an efficient wormhole detection algorithm in 3D wireless ad hoc networks by local topology detection. We introduce MaxIS (refer to Definition 1 in Section 3.3) into wormhole detection to recognize forbidden substructures in a certain covering area. The reason why we use MaxIS is that most efficient forbidden substructures are based on possible independence numbers $\alpha(G)$ (size of MaxIS) in certain topology graph *G*. If the detected $\alpha(G)$ is greater than a proper value (forbidden number), then it is assumed that there is a wormhole link around this local area.

Further more, in order to evaluate the effectiveness of various forbidden substructures, for the first time a physics theory named *distribution of distance in discs(spheres)* [13] is introduced into bound analysis on independence number $\alpha(G)$ in wireless ad hoc networks with a certain node density. Specifically, if possible $\alpha(G)$ in a covering area of a wormhole node is greater than the forbidden number, then MaxIS algorithm is very likely to find the wormhole link. Therefore, driven by above understandings, we discover an efficient forbidden substructures in 3D ad hoc networks and prove its effectiveness. The efficient forbidden structure is: 3 non-neighboring nodes have at most 2 independent common neighbors. Theoretical analysis show that both 2D and 3D forbidden substructures achieve 100% detection when the average degree of ad hoc networks is above 8, which means forbidden substructure based wormhole detection has a comparable performance in 2D and 3D. The main contributions of this paper can be summarized as follows:

(1) We introduce MaxIS into wormhole detection and propose some efficient forbidden substructures in 3D. Bound analysis on independence number $\alpha(G)$ in ad hoc networks is proposed for the first time and theoretically demonstrates the effectiveness of the forbidden substuctures.
(2) MaxIS-based wormhole detection algorithms for 3D wireless ad hoc networks are proposed. Evaluation results confirm the efficiency of our MaxIS-based algorithms in general communication model. For random distribution, the detection rate rises up to 100% even with poor network connectivity. Since forbidden substructures based wormhole detection has sound performance in 3D as it is in 2D, we can say that it performs well in any cases.

2. Preliminary

Existing forbidden substructures in wormhole detection are based on understandings of independence numbers in certain topology graphs. Before introducing MaxIS into this problem, in this section we review some previous works on forbidden substructure based wormhole detection. There are two major forbidden substructure based wormhole detection algorithms respectively proposed in [12] and [2]. We will review the main ideas of these two approaches. Notations used in this paper are illustrated in Table 1.

In homogeneous wireless networks, all nodes have the same transmission range. *Unit Disk Graph* (UDG) [14] is often used to abstract the networks on a 2-dimensional space, and *Unit Ball Graph* (UBG) [15] is used in 3-dimensional space. In most cases, people study wireless ad hoc and sensor networks in 2-dimensional space. They also assume that each node in wireless networks covers a circular area and use *Disk Graphs* (DG) to abstract the networks. But sometimes this assumption does not hold in reality. For example, *Underwater Sensor Networks* (USNs) consist of underwater autonomous vehicles distributed in 3-dimensional space [16]. Some other atmospheric or space communications are also apparent examples.

The basic idea of literature [12] is shown in Fig. 2. As depicted in Fig. 2, the wormhole attacks launched by two transceivers respectively at *A* and *B*. Nodes *b* and *c* are both neighbors of node *a* due to the existence of wormhole link. Thus, node *a* has two independent neighbors. Then, node *a* reduces its transmission range

Table 1
Notations.

$p(\mathcal{S})$	The packing number, which is the maximum number of vertices inside a region $\mathcal{S}$ such that every pair of vertices are strictly more than the unit distance from each other.
$\mathcal{D}(u)$	A unit disk centered at u.
$\mathcal{D}_r(u)$	A disk of radius r centered at u.
$\mathcal{B}(u)$	A unit ball centered at u.
$\mathcal{B}_r(u)$	A sphere of radius r centered at u.
$\mathcal{D}$	A unit disk.
$\mathcal{B}$	A unit ball.
$\mathcal{L}$	A lune. Given two unit disks centered at u and v with unit distance away, define by lune the intersection of two unit disks $\mathcal{D}(u)$ and $\mathcal{D}(v)$. As shown in Fig. 3(a)(b), $\mathcal{L} = \mathcal{D}(u) \cap \mathcal{D}(v)$.
$\mathcal{L}(r, R)$	A lune. Given two disks of radius R centered at u and v with distance r away, define by lune the intersection of two disks $\mathcal{D}_R(u)$ and $\mathcal{D}_R(v)$. $\mathcal{L}(r, R) = \mathcal{D}_R(u) \cap \mathcal{D}_R(v)$.
$\mathcal{H}$	A dish. Given two unit balls centered at u and v with unit distance away, define by dish the intersection of two unit balls $\mathcal{B}(u)$ and $\mathcal{B}(v)$. As shown in Fig. 5(a,c), $\mathcal{H} = \mathcal{B}(u) \cap \mathcal{B}(v)$.
$\mathcal{O}$	An olive. Given three unit balls centered at p, u and v with unit distance away, define by olive the intersection of three unit balls $\mathcal{B}(p)$, $\mathcal{B}(u)$ and $\mathcal{B}(v)$. As shown in Fig. 6(b), $\mathcal{O} = \mathcal{B}(p) \cap \mathcal{B}(u) \cap \mathcal{B}(v)$.
$arc - \mathcal{T}$	An arc-triangle. Given three unit disks centered at p, u, v with unit distance away, define by arc-triangle the intersection of the three disks. As shown in Fig. 3(a,c), $arc - \mathcal{T} = \mathcal{D}(p) \cap \mathcal{D}(u) \cap \mathcal{D}(v)$.
$camber - \mathcal{T}$	A camber-tetrahedron. Given four unit balls centered at v_1, v_2, u, v with unit distance away, define by camber-tetrahedron the intersection of the four balls. As shown in Fig. 6(c), $camber - \mathcal{T} = \mathcal{B}(v_1) \cap \mathcal{B}(v_2) \cap \mathcal{B}(u) \cap \mathcal{B}(v)$.
$N(u)$	Neighbors of a vertex u.
$N_k(u)$	k-hop neighbors of a vertex u.

r to $\frac{r}{2}$. If node a still finds two independent neighbors, a forbidden substructure is found. This forbidden substructure is based on the following observation: $\mathcal{D}_{\frac{r}{2}}(a)$ cannot contain two independent neighbors.

Notice that in 3D space a similar conclusion exists: $p(\mathcal{B}_{\frac{r}{2}}(u)) = 1$. Thus, wormhole detection algorithm in [12] actually holds in 3D.

Lemma 1. *In UDG, a disk of radius half the unit distance cannot contain two independent vertices.*

$$p(\mathcal{D}_{\frac{r}{2}}(u)) = 1$$

In UBG, a sphere of radius half the unit distance cannot contain two independent vertices.

$$p(\mathcal{B}_{\frac{r}{2}}(u)) = 1$$

where r is the unit distance. □

It should be noted that algorithm in [12] requires adjustable transmission radius. This is a strong requirement. Although we prove that algorithm in [12] is not limited in 2D, existing forbidden substructure based wormhole detection algorithms seldom consider 3D cases. For example, a forbidden substructure for UDG has been proposed in [2]. The basic idea in [2] is that there are at most 2 independent vertices existing in the common neighboring area between two independent vertices in UDG. In Lemma 2, we present a new proof which is different from [2]:

Lemma 2. *In UDG, a lune $\mathcal{L}$ contains at most two independent vertices.*

$$p(\mathcal{L}) = 2.$$

Proof. As shown in Fig. 3(c), an arc-triangle $arc - \mathcal{T}$ cannot contain two independent vertices:

$$p(arc - \mathcal{T}) = 1$$

The detailed proof is shown in Fig. 3(d). m' and n' are two vertices inside the $arc - \mathcal{T}$. m and n are intersection nodes of line $m'n'$ and arcs $\widehat{pu}$, $\widehat{pv}$. Line us is the perpendicular bisector of line segment vn. Thus,

$$|m'n'| \le |mn| \le |sm| + |sn| = |sm| + |sv| = |mv|$$

$|mv|$ is the unit distance. We have $p(arc - \mathcal{T}) = 1$. As shown in Fig. 3(b), $arc - \mathcal{T}_{puv}$ and $arc - \mathcal{T}_{quv}$ cannot contain two independent vertices respectively. Thus, there can only be two vertices inside $\mathcal{L}$ with inter distance larger than 1. This completes the proof. □

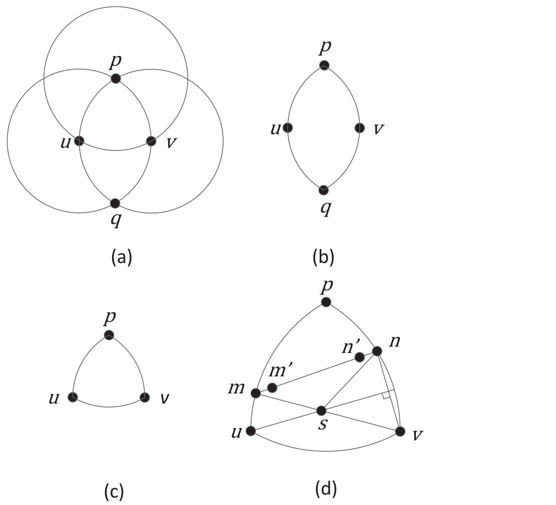


Fig. 3. As illustrated in the figure, p, u, v are three vertices with unit distance away. (a) shows three unit disks $\mathcal{D}(p)$, $\mathcal{D}(u)$ and $\mathcal{D}(v)$. (b) shows a lune $\mathcal{L}$. (c)(d) show an $arc - \mathcal{T}$.

As shown in Fig. 1, there are two independent vertices a, b in region w_0, then these two vertices share at most two common independent neighbors. However, vertices c, d, e are all recognized as neighbors of a, b since the wormhole link exists. Hence, the wormhole attack is detected. Furthermore, we can define the forbidden parameter in UDG:

$$f = p(\mathcal{L}) + 1 = 3$$

3. Wormhole detection algorithm

In Section 2, we introduce UDG and UBG models which are used to abstract the wireless networks. A natural idea is to check if the connectivity graph is a UDG(UBG) or not. If the connectivity graph has no valid UDG(UBG) embedding, it can be deduced that there must be a wormhole present in the network. However, finding a UDG(UBG) is NP-hard [17]. The basic idea in forbidden substructure based wormhole detection algorithm is to look for graph substructures that do not allow a UDG(UBG) embedding. As we mentioned before, forbidden substuctures detection in wireless ad hoc networks is based on the solution of MaxIS construction. In

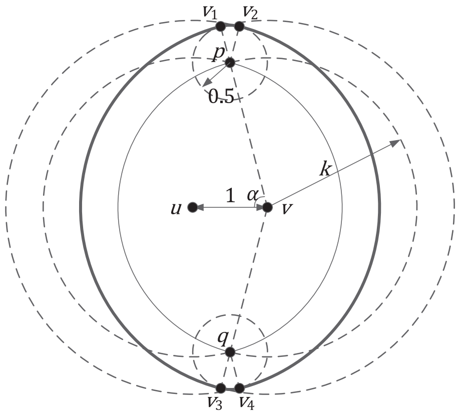


Fig. 4. On the proof on Theorem 1.

fact, performance bound analysis of approximation algorithms of MaxIS construction reduce to *circle* or *sphere packing problems* in wireless ad hoc networks [18].

3.1. Circle packing and forbidden substructures

In Lemma 2, a forbidden substructure is presented. Literature [2] generalizes the result for packing of circles of radius *k*. However, only a loose bound is given in [2]. In this paper, we present better theoretical analysis of this circle packing problem and give tighter upper bounds.

As shown in Fig. 4, our goal is to calculate the maximum number of independent vertices that contained in $\mathcal{L}(1,k)=\mathcal{D}_k(u)\cap\mathcal{D}_k(v)$. This is a circle packing problem. Thus, calculating the packing number in $\mathcal{L}(1,k)$ becomes to find the maximum number of congruent circles of radius 0.5 that can be packed in the area enclosed by heavy solid lines. Notice that arc $\widehat{v_1v_2}$ belongs to the circle of radius 0.5 centered at p, arc $\widehat{v_3v_4}$ belongs to the circle of radius 0.5 centered at q.

For a convex domain, we have the following lemma in [19]:

Lemma 3. *If n is the number of the unit circles (of radius 1) packed in a convex domain Q, then:*

$$n\sqrt{12}\leq A(Q)-\frac{2-\sqrt{3}}{2}P(Q)+\sqrt{12}-\pi(\sqrt{3}-1)$$

where A(Q) is the area of domain Q, P(Q) is the perimeter of domain Q. □

Theorem 1.

$$p(\mathcal{L}(1,k))\leq(\frac{4}{3}\sqrt{3}k^2+2k)arccos\frac{1}{2k}-\frac{2}{3}\sqrt{3}\sqrt{k^2-0.25}+1$$

Proof. As shown in Fig. 4, u and v are two adjacent vertices in UDG. We assume that $|uv|=1$. p and q are intersection vertices of $\mathcal{D}_k(u)$ and $\mathcal{D}_k(v)$. v_1, v_3 are intersection vertices of line pv, qv and $\mathcal{D}_{(k+0.5)}(v)$. v_2, v_4 are intersection vertices of line pu, qu and $\mathcal{D}_{(k+0.5)}(u)$. Denote the convex domain enclosed by heavy solid lines $domain_{v_1v_2v_4v_3}$. Since domain enclosed by $\widehat{v_1v_2}$, $\widehat{v_2v_4}$, $\widehat{v_4v_3}$, $\widehat{v_3v_1}$ is convex, through Lemma 3, we have

$$\begin{aligned}p(\mathcal{L}(1,k))\leq&\frac{\sqrt{3}}{6}A(domain_{v_1v_2v_4v_3})\cdot 4\\&-\frac{2\sqrt{3}-3}{12}P(domain_{v_1v_2v_4v_3})\cdot 2+1\\&-\pi\frac{3-\sqrt{3}}{6}\end{aligned}$$

Thus,

$$\begin{aligned}A(domain_{v_1v_2v_4v_3})=&A(sector_{vv_1v_3})+A(sector_{uv_2v_4})\\&-A(parallelogram_{puqv})\\&+A(sector_{pv_1v_2})+A(sector_{qv_3v_4})\end{aligned}$$

$$P(domain_{v_1v_2v_4v_3})=|\widehat{v_1v_2}|+|\widehat{v_2v_4}|+|\widehat{v_4v_3}|+|\widehat{v_3v_1}|$$

Denote $\angle pvu=\angle\alpha$, thus, $\angle v_1pv_2=\pi-2\angle\alpha$,

Since line pq is the perpendicular bisector of line segment uv, we have

$$\angle\alpha=arccos\frac{\frac{1}{2}|uv|}{|pv|}=arccos\frac{1}{2k}$$

Thus, with some algebraic steps, we have

$$p(\mathcal{L}(1,k))\leq(\tfrac{4}{3}\sqrt{3}k^2+2k)\cdot arccos\tfrac{1}{2k}-\tfrac{2}{3}\sqrt{3}\sqrt{k^2-0.25}+1$$

This completes the proof. □

Upper bounds for $p(\mathcal{L}(1,k))$ is tighter because we use Lemma 3. Upper bounds for $p(\mathcal{L}(1,k))$ in [2] is loose because their method is too simple:

$$p(\mathcal{L}(1,k))\leq\frac{A(\mathcal{L}(1,k+0.5))}{A(\mathcal{D}_{0.5}(p))}$$

It is claimed in [2] that *k*-hop detection performs better than 1-hop only detection in non-UDG cases. But it should be noted that maintaining more than 1-hop neighbor information for each node incurs extra overhead of the system and the information can hardly be accurate when the mobility of the system is high. To this end, we focus on 1-hop detection in this paper.

Theorem 2. *In UDG, a circle of radius* 0.5*r*, 0.5773*r*, 0.7071*r and* 0.8506*r contains at most 1,2,3 and 4 independent vertices.*

$$p(\mathcal{D}_{0.5r}(u))=1$$

$$p(\mathcal{D}_{0.5773r}(u))=2$$

$$p(\mathcal{D}_{0.7071r}(u))=3$$

$$p(\mathcal{D}_{0.8506r}(u))=4$$

where r is the unit distance.

Proof. In circle packing problem, there are at most 1,2,3,4 unit disks inside a disk of radius 0.5*r*, 0.5773*r*, 0.7071*r* and 0.8506*r* [20].

This completes the proof. □

From Theorem 2, we can define the forbidden parameter in delay tolerant networks:

$$f^*=p(\mathcal{D}_R(u))+1$$

where $R\in\{0.5r, 0.5773r, 0.7071r, 0.8506r\}$.

3.2. Sphere packing and forbidden substructures

Lemma 4. *In UBG, a camber-tetrahedron camber* $-\mathcal{T}$ *cannot contain two independent vertices.*

$$p(camber-\mathcal{T})=1$$

Proof. The proof is similar to Lemma 2. Every two vertices in the area have distance at most 1.

This completes the proof. □

Similar to Lemma 2, our main idea is that there must be a tight upper bound for the number of independent vertices can be contained in the common neighboring area between two independent vertices in UBG.

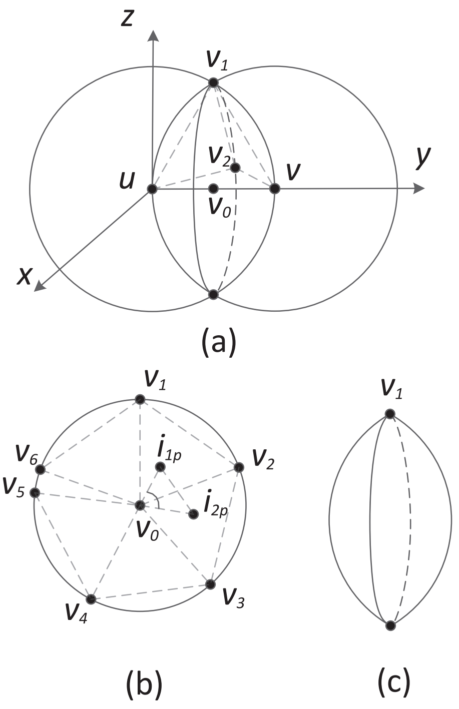


Fig. 5. As illustrated in the figure, u, v are two vertices with unit distance away. (a) shows two unit balls $\mathcal{B}(u)$, $\mathcal{B}(v)$. The intersection of two balls $\mathcal{B}(u)\cap\mathcal{B}(v)$ is a dish. (b) shows the circular edge of the dish $\mathcal{H}$. (c) shows the dish $\mathcal{H}$.

Theorem 3. *In UBG, a dish contains at most 5 independent vertices.*

$$p(\mathcal{H}) = 5$$

Proof. As shown in Fig. 5, u and v are two adjacent vertices in UBG. We assume that $|uv| = 1$. v_1 and v_2 are two vertices lying on the intersection circle of two spherical surfaces which centered at u and v. Assume that $|v_1v_2| = 1$. Thus,

$$|uv| = |uv_1| = |uv_2| = |v_1v_2| = |vv_1| = |vv_2| = 1$$

These four vertices u, v, v_1, v_2 constitute a tetrahedron.

As illustrated in Lemma 2, a camber-tetrahedron cannot contain two independent vertices. Thus, two independent vertices cannot be contained in *camber* $- \mathcal{T}_{uvv_1v_2}$.

Denote v_0 the mid-point of u and v, $Disk_{v_0}$ the disk centered at v_0, the boundary of $Disk_{v_0}$ is the intersection circle of two spherical surfaces.

Thus, if there exist two independent vertices i_1 and i_2 in the dish in Fig. 5, then the distance between their projections i_{1p} and i_{2p} on the disk $Disk_{v_0}$ must be greater than 1.

The radius of $Disk_{v_0}$ is $\frac{\sqrt{3}}{2}$. Thus, as shown in Fig. 5(b),

$$|v_0i_{1p}| \leq \frac{\sqrt{3}}{2}$$

$$|v_0i_{2p}| \leq \frac{\sqrt{3}}{2}$$

$$|i_{1p}i_{2p}| > 1$$

Thus,

$$\angle i_{1p}v_0i_{2p} > 2arcsin\frac{\sqrt{3}}{3}$$

$$\frac{2\pi}{\angle i_{1p}v_0i_{2p}} < \frac{2\pi}{2arcsin\frac{\sqrt{3}}{3}} \approx 5.1$$

This completes the proof. □

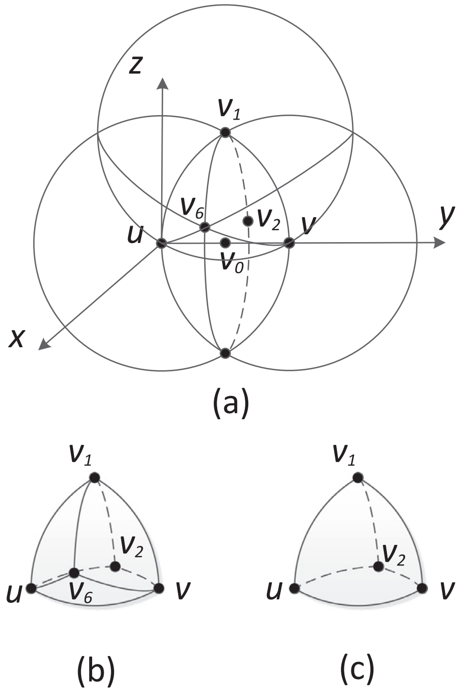


Fig. 6. As illustrated in the figure, u, v, v_1, v_2 are four vertices with unit distance away; u, v, v_1, v_6 are four vertices with unit distance away. (a) shows three unit balls $\mathcal{B}(u)$, $\mathcal{B}(v)$, $\mathcal{B}(v_1)$. v_2, v_6 are intersection points of the surfaces of these three unit balls. The intersection of three balls $\mathcal{B}(u)\cap\mathcal{B}(v)\cap\mathcal{B}(v_1)$ is an olive $\mathcal{O}$. (b) shows the olive $\mathcal{O}$. The intersection of four balls $\mathcal{B}(u)\cap\mathcal{B}(v)\cap\mathcal{B}(v_1)\cap\mathcal{B}(v_2)$ is a *camber* $- \mathcal{T}$. (c) shows the *camber* $- \mathcal{T}$.

From Theorem 3, we can define the forbidden parameter in UBG:

$$f = p(\mathcal{H}) + 1 = 6$$

Thus, in UBG, if two independent vertices have 6 or more common independent neighbors, then the wormhole attack is detected.

Theorem 4. *In UBG, an olive contains at most 2 independent vertices.*

$$p(\mathcal{O}) = 2$$

Proof. As shown in Fig. 6, u, v and v_1 are three adjacent vertices in UBG. We assume that

$$|uv| = |uv_1| = |v_1v| = 1$$

v_2, v_6 are intersection points of the surfaces of these three unit balls $\mathcal{B}(u)$, $\mathcal{B}(v)$, $\mathcal{B}(v_1)$. The intersection of three balls $\mathcal{B}(u)\cap\mathcal{B}(v)\cap\mathcal{B}(v_1)$ is an olive $\mathcal{O}$.

Thus,

$$|uv| = |uv_1| = |uv_2| = |v_1v_2| = |vv_1| = |vv_2| = 1$$

$$|uv| = |uv_1| = |uv_6| = |v_1v_6| = |vv_1| = |vv_6| = 1$$

Four vertices u, v, v_1, v_2 constitute a tetrahedron.

Four vertices u, v, v_1, v_6 constitute a tetrahedron.

As illustrated in Lemma 2, a camber-tetrahedron cannot contain two independent vertices. Thus, three independent vertices cannot be contained in $\mathcal{O}$.

This completes the proof. □

From Theorem 4, we can define the forbidden parameter in UBG:

$$f = p(\mathcal{O}) + 1 = 3$$

The discovery of this forbidden substructures reveals the existence of a wormhole. In UBG, if three independent vertices have 3 or more common independent neighbors, then the wormhole attack is detected.

3.3. MaxIS-based wormhole detection algorithm

Definition 1. Maximal independent set (MIS). Maximum independent set (MaxIS).

In graph theory, an independent set is a set of vertices in a graph G, such that no two of which are adjacent. Moreover, an MIS is an independent set that is not a subset of any other independent set. A MaxIS is an independent set of largest possible size for a given graph G. This size is called the independence number of G, and denoted $\alpha(G)$.□

Our wormhole detection algorithm is to search by each vertex a forbidden substructure in its neighborhood. Assume that u and v are two non-neighboring vertices. Notice that to find a non-empty set $N(u) \cap N(v)$, node u only needs to look for v in its 2-hop neighbors. Thus, each vertex in UDG or UBG maintains the neighboring list of neighbors within 2-hops. Then, we need to compute the size of MaxIS among $N(u) \cap N(v)$ and compare the size of this set with the forbidden parameter f.

That is, the forbidden substructure based wormhole detection reduces to MaxIS problem in UDG and UBG. Computing the MaxIS in UDG or UBG is an NP-hard problem [21,22]. A simple greedy algorithm for MIS problem is used in [2]. However, this is a misunderstanding about the MaxIS and MIS problems. The simple greedy algorithm for MIS cannot guarantee the large size of MaxIS. Since independence number $\alpha(G)$ of a graph is hard to find, our purpose is to find an MIS with a large size. Although finding a MaxIS is a classic problem, there is seldom feasible approximation algorithm proposed in recent years. Therefore, an effective approximation algorithm for MaxIS [23] is used in this paper. We name this effective approximation algorithm the improved greedy algorithm. The improved greedy algorithm forms a MaxIS by, at each step, choosing the minimum degree vertex in the graph and removing its neighbors. The algorithm achieves an approximation ratio of $(\Delta + 2)/3$, where $\triangle$ is the average degree of the nodes.

An example is shown in Fig. 7. u and v are two independent nodes. Thus, they have at most two common neighbors. Due to the existence of the wormhole link between A and B, $\mathcal{D}(u) \cap \mathcal{D}(v)$ and $\mathcal{D}(B)$ are both mistakenly recognized as the common neighboring area of u and v. It must be noted that, every pair of node in $\mathcal{D}(u) \cap \mathcal{D}(v)$ and node in $\mathcal{D}(B)$ think that they are neighbors of each other. Thus, we only need to study how to compute a MaxIS for nodes in $\mathcal{D}(B)$. As the figure shows, initially, all nodes are colored white. If a node is chosen as a member of the MaxIS in each step, it is colored black, and all its neighbors are colored grey. The degree of each node is labeled on the top. As the figure shows, the closer the vertex to the border of the disk, the lower degree the vertex has. In the simple greedy algorithm, each node has an equal chance to be selected as a member of the independent set. Hence, if vertices with degree 5 or 7 close to the center of the disk are selected as early on, the resulted MaxISs have very small sizes. Especially when the vertex with degree 7 is selected at the first step, the resulted MaxIS has only one element in it. Therefore, it is significantly important to use the improved greedy algorithm instead of simple greedy algorithm to detect the existence of forbidden substructures.

We present the outline of our wormhole detection algorithms in Algorithms 1 and 2 . Since the proposed algorithms are localized, message and time complexity of these two algorithms are dependent on the degree of nodes in the network. The time complexity of Algorithm 1 and Algorithm 2 is $O(\triangle^4)$, where $\triangle$ is the average degree of the nodes. That is, a node checks all of its $(\triangle^2)$ 2-hop non-neighboring nodes. In addition, each node pays a cost of $O(\triangle^2)$ for finding the approximate solution of the size of MaxIS. For practical wireless ad hoc networks, $\triangle$ is generally a small constant, so that the proposed wormhole detection algorithms are efficient.

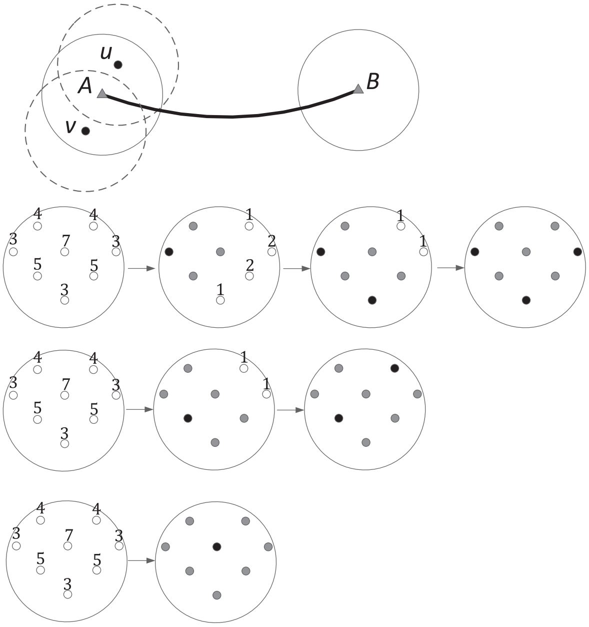


Fig. 7. $\mathcal{D}(u) \cap \mathcal{D}(v)$ and $\mathcal{D}(B)$ are both mistakenly recognized as the common neighboring area of u and v. Every node in $\mathcal{D}(u) \cap \mathcal{D}(v)$ and node in $\mathcal{D}(B)$ think that they are neighbors of each other. Thus, we only need to study how to compute a maximum independent set for nodes in $\mathcal{D}(B)$.

Algorithm 1: Wormhole detection with Lemma 1 and Theorem 3.

```
Input: Node $u$.
Output: $W \in \{0, 1\}$(Represent the existence of wormholes).
Initialized to $W = 0$.
for each $v \in N_2(u)$ do
    $u$ requests $v$ to send $N(v)$ to $u$, $S = N(u) \cap N(v)$.Compute a
    MaxIS $\mathcal{M}$ of $G_S$, where $G_S$ is the subgraph on $S$.
    if $|\mathcal{M}| \geq f$ then
        $W = 1$
```

Algorithm 2: Wormhole detection with Theorem 4.

```
Input: Node $u$.
Output: $W \in \{0, 1\}$(Represent the existence of wormholes).
Initialized to $W = 0$.
for each $v \in N_2(u)$ do
    Let $N_2(u)' = N_2(u)$.
    $u$ requests $v$ to send $N_2(v)$ to $u$, $S = N_2(u)' \cap N_2(v)$.
    for each $p \in S$ do
        $u$ requests $p$ to send $N(p)$ to $u$, $T = N(p) \cap N(u) \cap N(v)$.
        Compute a MaxIS $\mathcal{M}$ of $G_S$, where $G_S$ is the subgraph
        on $T$.
        if $|\mathcal{M}| \geq f$ then
            $W = 1$
        $S = S \setminus p$
    if $S = \varnothing$ then
        $N_2(u)' = N_2(u)' \setminus v$
```

Wormhole removal will be the main concern once a forbidden substructure is discovered. A simple wormhole removal approach is proposed in [2]. In this paper we adopt the similar approach and make a brief description of it. As it is depicted in Section 4 and Section 5, Algorithm 1 with Theorem 4 has better performance than Algorithm 1 with Theorem 3. Therefore, we only present the wormhole removal approach for Algorithm 2. Firstly, we define two types of nodes neighboring the wormhole region, the corrupted nodes and uncorrupted nodes. Once the forbidden substructure is found by three non-neighboring nodes *a, b* and *c* with three common independent neighbors *d, e* and *f*, two sets of corrupted nodes C_1 and C_2 are defined as:

(1) C_1 is the set in which a node is neighbor of at least 2 nodes out of *a, b* and *c*.
(2) C_2 is the set in which a node is neighbor of at least 2 nodes out of *d, e* and *f*.

Moreover, a link between a pair of corrupted nodes in C_1 and C_2 is considered as a wormhole link. All future transmissions through such links will be ignored. In this process, some legal links may be removed inevitably.

3.4. General communication model and node mobility

In previous sections, several forbidden substructures in UDG and UBG have been given. As two typical models for wireless communications, discussions about forbidden numbers in UDG and UBG reveal the essence of forbidden substructure based wormhole detection algorithm. However, UDG and UBG models are too idealistic, overly simplified and might not be applicable in reality. Thus, considerations of different communication models and node distribution are important. Fortunately, forbidden substructure based wormhole detection algorithm can be generalized to any communication model and performs well [2]. The algorithm indeed remains the same. But it is needed to tune the forbidden number according to the specific communication model and node mobility.

For general communication model, similar technique to obtain the forbidden number in [2] is used in this paper. We run the detection algorithm with a standard parametric search for the forbidden substructures. We start with a large initial value for the forbidden number *f*, and run the algorithm as presented before. If no wormhole is detected, we have *f* and rerun the algorithm. The weakness of this technique is that in order to ensure high detection rate, false positives are inevitable in certain cases. However, simulation results in Section 5 show that the error rate is extremely low.

We also propose Algorithm 3 for delay tolerant networks, which are emerged from mobile ad hoc networks (MANETs) [24]. Unlike Algorithms 1 and 2, we assume that the transmission range of nodes is adjustable. The time complexity of Algorithm 3 is $O(\triangle^3)$. Delay tolerant networks lack continuous network connectivity and instantaneous end-to-end paths are difficult to establish. To this end, mobility model (such as Random Way Point [25] or Zebranet [26]) is an essential factor in evaluating routing protocols for delay tolerant networks. Compared with Algorithms 1 and 2, Algorithm 3 does not need two nodes to exchange their neighboring information. However, a node has to reset its transmission range when it decides to detect the existence of a wormhole attack.

Algorithm 3: Wormhole detection with Theorem 2.

```
Input: Node $u$.
Output: $W \in \{0, 1\}$(Represent the existence of wormholes).
Initialized to $W = 0$.
for each $R \in \{0.5r, 0.5773r, 0.7071r, 0.8506r\}$ do
    $u$ resets its transmission range to $R$.
    $S = N(u)$.
    Compute a MaxIS $\mathcal{M}$ of $G_S$, where $G_S$ is the subgraph on $S$.
    if $|\mathcal{M}| \geq f^*$ then
        $W = 1$
```

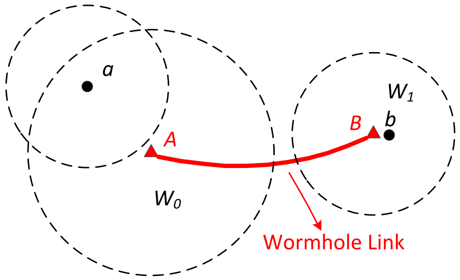


Fig. 8. In heterogeneous wireless networks, as shown in the figure, a simple way to detect the wormhole link is that node *a* broadcasts to all its neighbors and sees if it can get responses from *b*.

Table 2
Forbidden substructures.

	Model	Number of independent nodes f'	Forbidden number f
Rule 1	*UDG*	1	≥ 6
Rule 2	*UDG*	2	≥ 3
Rule 3	*UDG*	3	≥ 2
Rule 4	*UBG*	1	≥ 13
Rule 5	*UBG*	2	≥ 6
Rule 6	*UBG*	3	≥ 3
Rule 7	*UBG*	4	≥ 3
Rule 8	*UBG*	5	≥ 3

4. Performance analysis

Next, we will explain the reason why some forbidden substructures are more efficient than others for detection of wormhole. To answer this question, we first explain why adversaries generally launch wormhole attacks in homogeneous networks. A simple fact is that a smart attacker uses homogeneous malicious nodes which have the same transmission range as transmission range of the nodes in wireless networks. As shown in Fig. 8, If *A* has a larger transmission range, node *a* receives messages from node *b* when node *b* cannot receive messages from node *a*. Thus, a simple way to detect the wormhole link is that node *a* broadcasts to all its neighbors and sees if it can get responses. In some cases, the adversary may replicate captured sensors and deploy them in the network to launch another variety of malicious activity which is referred to as the clone attack [27,28]. Then cloned nodes can launch wormhole attacks.

The forbidden substructures presented in previous section are not the only forbidden substructures in UDG and UBG. Actually other characteristics for UDG(UBG) also can be used as forbidden substructures. We already have $p(\mathcal{L}) = 2$, which means in UDG, forbidden number for 2 independent nodes is 3. As shown in Fig. 3(a), 3 independent nodes share no more than 1 independent neighbor. We summarize these forbidden substructures of Lemmas 1, 2, Theorems 3 and 4 in Table 2. Rule 1 ($p(\mathcal{D}) = 5$) and Rule 4 ($p(\mathcal{B}) = 12$) can be found in [15,18,29]. Notice that Rule 2 and Rule 3 are equivalent for wormhole detection.

To figure out which one of them is more efficient for wormhole detection, we need to clarify how does wormhole influence the nodes covered by it. As shown in Fig. 7, efficiency of a forbidden substructure mainly depends on two aspects: 1. Probability of the existence of f' (in Table 2) independent nodes in a unit disk(sphere); 2. Probability of the existence of f independent nodes in a unit disk(sphere). To solve this problem, we put forward the following question:

How to find the probability density $P(l)$ for the distance l between points in a circle(sphere) of radius r?

The answer has been given in [13]:

$$P(l) = \frac{4l}{\pi r^2} arccos \frac{l}{2r} - \frac{2l^2}{\pi r^4}\sqrt{r^2 - \frac{l^2}{4}}$$

Lemma 5. *The probability density P for the distance l between points in a unit circle is:*

$$P(l) = \frac{4l}{\pi} arccos \frac{l}{2} - \frac{2l^2}{\pi}\sqrt{1 - \frac{l^2}{4}}$$

The probability density P for the distance l between points in a unit sphere is:

$$P(l) = \frac{3}{16}(l-2)^2 l^2 (l+4)$$

Thus, the probability that two nodes in a unit circle are independent to each other is:

$$1 - \int_0^1 P(l)dl = 1 - \int_0^1 \left(\frac{4l}{\pi} arccos \frac{l}{2} - \frac{2l^2}{\pi}\sqrt{1 - \frac{l^2}{4}}\right)dl$$

$$= \frac{3\sqrt{3}}{4\pi} \approx 0.4135$$

The probability that k nodes in a unit circle are independent to each other is upper bounded by:

$$\left(1 - \int_0^1 P(l)dl\right)^{C_k^2} = \left(\frac{3\sqrt{3}}{4\pi}\right)^{C_k^2}$$

Denote the average degree of the network is Δ. Thus, each node has an average of Δ neighbors. Each wormhole transceiver covers an average of Δ nodes. The probability that among these Δ nodes, there exist k nodes independent of each other is upper bounded by:

$$P_{UDG}{}_{\Delta}^{k} = 1 - \left(1 - \left(\frac{3\sqrt{3}}{4\pi}\right)^{C_k^2}\right)^{C_\Delta^k}$$

Similarly, the probability that two nodes in a unit sphere are independent to each other is:

$$1 - \int_0^1 P(l)dl = 1 - \int_0^1 \left(\frac{3}{16}(l-2)^2 l^2 (l+4)\right)dl$$

$$= \frac{17}{32} \approx 0.5313$$

The probability that k nodes in a unit circle are independent to each other is upper bounded by:

$$\left(1 - \int_0^1 P(l)dl\right)^{C_k^2} = \left(\frac{17}{32}\right)^{C_k^2}$$

Inside a covering area of a wormhole transceiver, the probability that among Δ nodes, there exist k nodes independent of each other is upper bounded by:

$$P_{UBG}{}_{\Delta}^{k} = 1 - \left(1 - \left(\frac{17}{32}\right)^{C_k^2}\right)^{C_\Delta^k}$$

Thus, for example, as shown in Table 2, the performance of Rule 2 can be defined as follows:

$$P_{UDG}{}_{\Delta}^{f'} \cdot P_{UDG}{}_{\Delta}^{f} = P_{UDG}{}_{\Delta}^{2} \cdot P_{UDG}{}_{\Delta}^{3}$$

The performance of all the rules in Table 2 is shown in Figs. 9 and 10. Notice that Rule 6 has the best performance in all these rules.

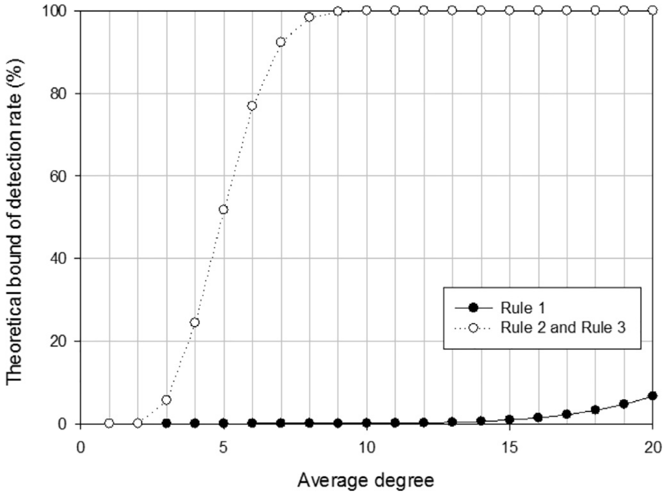


Fig. 9. The theoretical detection rate of forbidden substructures $p(\mathcal{L}) = 2$ (Rule 2) in UDG is illustrated.

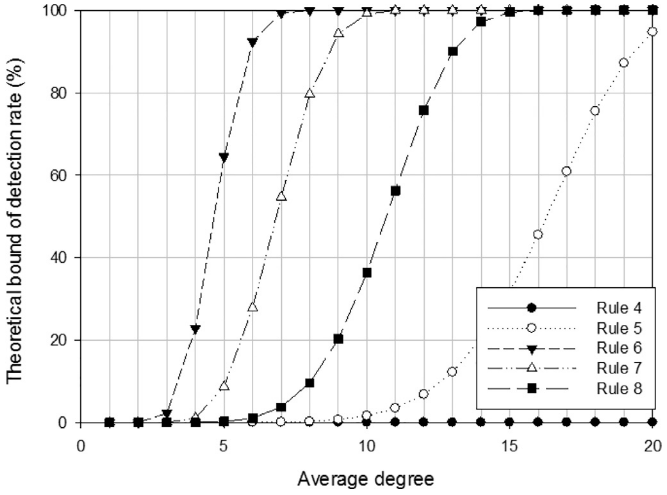


Fig. 10. The theoretical detection rate of forbidden substructures $p(\mathcal{O}) = 2$ (Rule 6), $p(\mathcal{H}) = 5$ (Rule 5) in UBG is illustrated.

5. Evaluation results

We conduct extensive simulations under various situations to evaluate the effectiveness of our approach. Firstly, we evaluate the probability of successful detection for networks with various node densities. We consider three different connectivity models in our simulations: UDG, UBG, quasi-UBG; nodes are deployed using two models: random placement and perturbed grid; three forbidden substructures: $p(\mathcal{L}) = 2,\ p(\mathcal{H}) = 5,\ p(\mathcal{O}) = 2$; two MaxIS construction algorithms: the simple greedy algorithm and the improved greedy algorithm. Secondly, we evaluate the performance of our algorithm for delay tolerant networks. We consider UDG model; four forbidden substructures: $p(\mathcal{D}_{\frac{r}{2}}(u)) = 1,\ p(\mathcal{D}_{0.5773r}(u)) = 2,\ p(\mathcal{D}_{0.7071r}(u)) = 3$ and $p(\mathcal{D}_{0.8506r}(u)) = 4$; the improved greedy algorithm for MaxIS construction.

5.1. Simulation setup

We carried out extensive simulations using the network simulator ns-3 (version 3.26) to test the performance of the proposed algorithms. The MAC layer follows the 802.11 MAC specification. The popular two-ray ground reflection model is adopted as the ra-

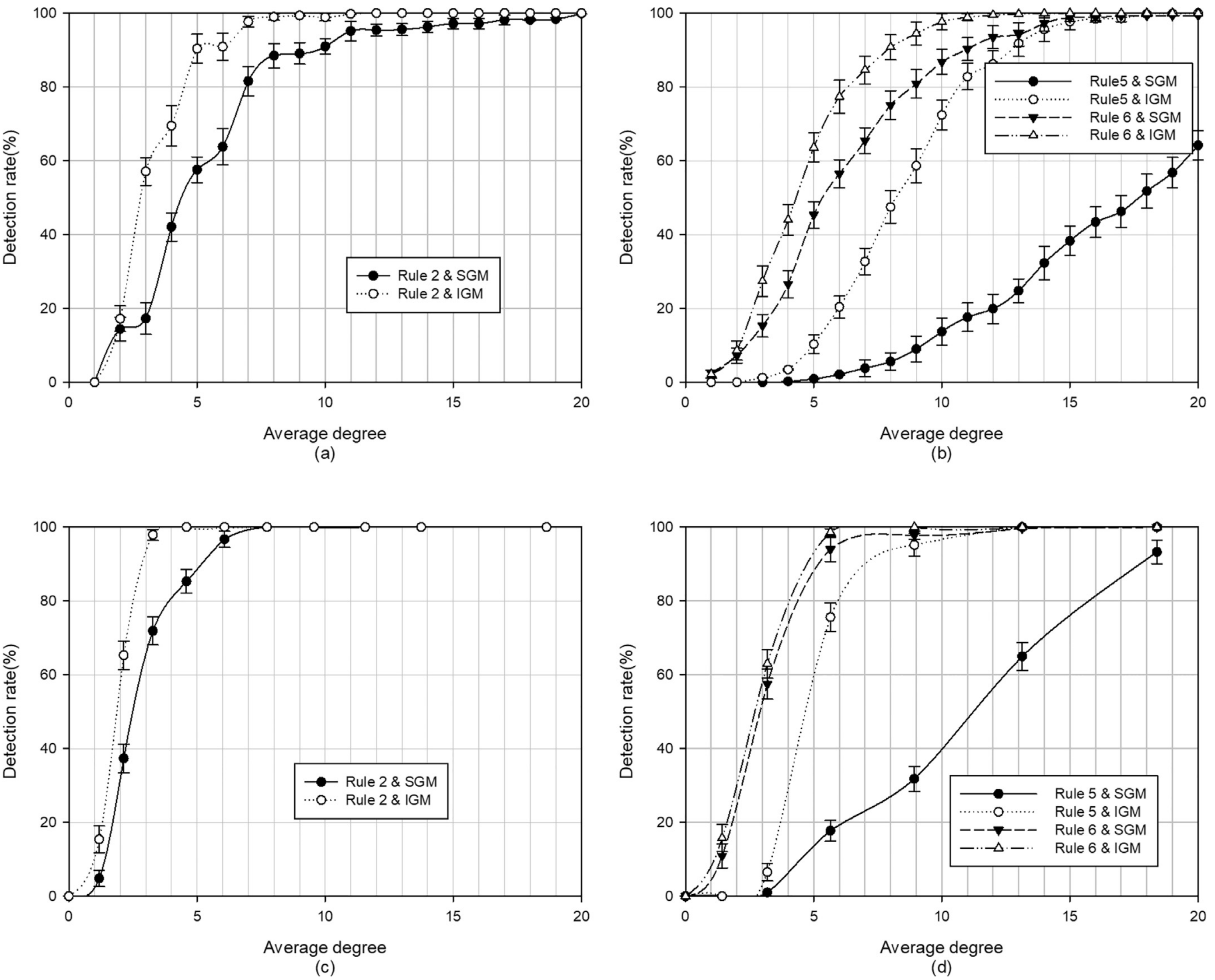


Fig. 11. Probability of wormhole detection. (a) and (b) are for Random node distribution. (c) and (d) are for a Perturbed Grid node distribution. (a) and (c) are for $p(\mathcal{L}) = 2$ with UDG model. (b) and (d) are for $p(\mathcal{H}) = 5,\ p(\mathcal{O}) = 2$ with UBG model. SGM denotes simple greedy maximum independent set construction. IGM denotes improved greedy maximum independent set construction. Both simple and improved greedy maximum independent set constructions are tested.

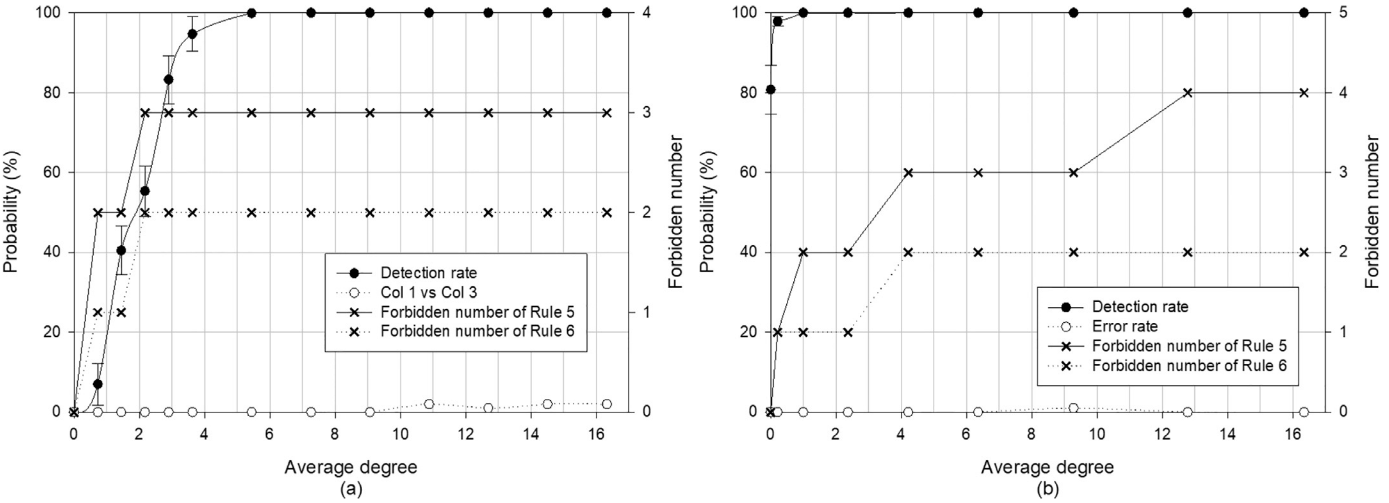


Fig. 12. Probability of wormhole detection and estimation of the forbidden number in quasi-UBG. (a) is for Random node distribution. (b) is for a Perturbed Grid node distribution. The forbidden numbers are tested for Rule 5 and Rule 6, when the number f' of independent nodes is 2 or 3.

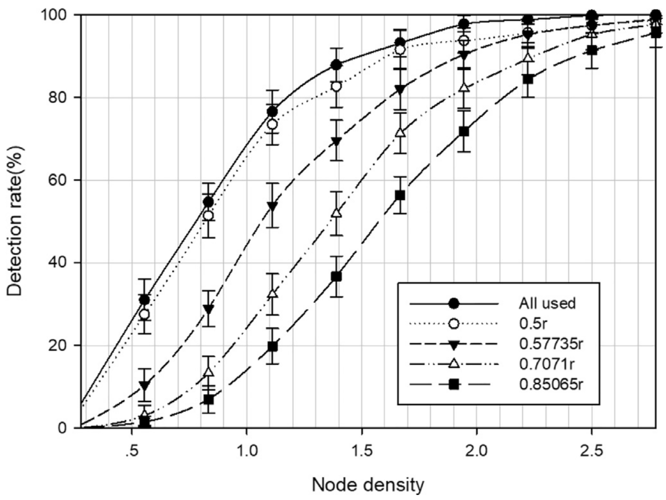


Fig. 13. The wormhole detection rate in delay tolerant networks. The performances of forbidden substructures $p(\mathcal{D}_{0.5773r}(u))$, $p(\mathcal{D}_{0.8506r}(u))$ and a combination of $p(\mathcal{D}_{\frac{r}{2}}(u))$, $p(\mathcal{D}_{0.5773r}(u))$, $p(\mathcal{D}_{0.7071r}(u))$, $p(\mathcal{D}_{0.8506r}(u))$ are illustrated.

dio propagation model. The bandwidth of a wireless channel is set to 2 Mb/s.

Firstly, we use UDG and UBG model to build the network and evaluate the algorithm with perturbed grid (modeling a planned sensor deployment) and random distribution. We vary the transmission radius of sensors to yield average node degrees from 1 to 20. For each set of simulation, we conduct 1000 runs with different node generations and report the average. Secondly, quasi-UBG model is used to test the performance of our algorithms in non-UDG(UBG) cases. In quasi-UBG model, suppose the transmission range of nodes is R and the quasi-UBG factor is set to α, then for a pair of nodes, 1) if the distance between them is smaller than αR, there exists a link between them, and 2) if the distance d between them is within $[\alpha R, R]$, the probability that there exists a link between is $d/(R-\alpha R)$. In our simulation α is set to 0.75. Moreover, for delay tolerant networks, we use UDG to build the network and evaluate the algorithm with the mobility model of Random Way Point. The nodes are deployed in a $1000 \times 1000\,\text{m}^2$ region and the transmission range of nodes is set to 100 m. The node density is defined as the average number of nodes inside a $100\,\text{m}^2$ region. We test the detection rate under different node densities.

5.2. Results

As shown in Fig. 11, simulation results are consistent with the theoretical results. Simulation results show that the improved greedy algorithm for MaxIS construction greatly improves the wormhole detection rate.

As shown in Fig. 11(a), if the simple greedy algorithm in [2] is used, the detection rate rises up to 100% when the average node degree is above 20. If the improved greedy algorithm in this paper is used, the detection rate rises up to almost 100% when the average node degree is above 8. As it shown in simulation results given in [10], their fundamental topology deviations based approach does not perform well in random node deployment because of the poor connectivity. For the random deployment, their detection rate approaches 100% when the average node degree increases to 18. For the perturbed grid model, their detection rate approaches 100% when the average node degree is above 8. As shown in Fig. 11(c), for the perturbed grid model, our detection rate approaches 100% when the average node degree is above 4. Thus, wormhole detection approach proposed in this paper is much better than existing approaches.

Fig. 11(b) and (d) shows the simulation results in 3D. As shown in Fig. 11(b) and (d), we compare the wormhole detection rates when forbidden substructures $p(\mathcal{H}) = 5$ and $p(\mathcal{O}) = 2$ are used. The results show that wormhole detection algorithm based on forbidden substructure $p(\mathcal{O}) = 2$ is much better. The improved greedy MaxIS construction algorithm still shows its advantage in 3D. For the random deployment, if Algorithm 1 and the improved greedy algorithm are both used, the detection rate rises up to 100% when the average node degree is above 18. If Algorithm 2 and the improved greedy algorithm are both used, the detection rate rises up to 100% when the average node degree is above 12. This is the packing number in a Unit Ball, which means that the forbidden substructure based wormhole detection approach achieves sound performance in 3D. Even when the average degree is 8, our approach has detected the wormhole attack in 90% or more cases.

Fig. 12(a) and (b) shows the simulation results in quasi-UBG. Fig. 12 also shows values of the forbidden number f in different node distributions. As shown in the Fig. 12(a), for random distribution, the detection rate rises up to 100% when average node degree is above 6. When average node degree is above 10, although the detection rate is still 100%, false positives show up. As shown in Fig. 12(b), for perturbed grid distribution, the detection rate rises up to 100% when average node degree is above 2. Very low error rate shows when the average node degree is around 9. Simulation results show that Algorithms 1 and 2 are quite efficient in non-UDG cases, but in certain cases uncertain parameter f leads to false positives. To this end, we think forbidden substructure based wormhole detection experiment for quasi-UDG in [2] is correct and sufficient.

Fig. 13 shows the simulation results in delay tolerant networks. As depicted in Fig. 13, we first compare the wormhole detection rates of four forbidden substructures $p(\mathcal{D}_{0.5r}(u))$, $p(\mathcal{D}_{0.5773r}(u))$, $p(\mathcal{D}_{0.7071r}(u))$ and $p(\mathcal{D}_{0.8506r}(u))$. The results show that the performance of $p(\mathcal{D}_{0.5r}(u))$ is better. When the node density is 1.39, the detection rates of $p(\mathcal{D}_{0.5r}(u))$ and $p(\mathcal{D}_{0.8506r}(u))$ are 83% and 37%. Moreover, the wormhole detection rate can be further improved by using more forbidden substructures. If all four forbidden substructures $p(\mathcal{D}_{0.5r}(u)) = 1$, $p(\mathcal{D}_{0.5773r}(u)) = 2$, $p(\mathcal{D}_{0.7071r}(u)) = 3$, $p(\mathcal{D}_{0.8506r}(u)) = 4$ are used, the detection rates rise up to 88% and 100% when the node densities are 1.39 and 2.5.

6. Conclusion

Wormhole attack is a severe threat to wireless ad hoc networks. In this paper we proposed a localized wormhole attack detection approach in 3D wireless ad hoc networks based on forbidden substructures. Detailed theoretical analysis illustrate the existence of efficient forbidden substructures in 3D space. Especially, the sound performance of forbidden substructure based wormhole detection algorithms is not limited by the communication and mobility model. The approach is lightweight and easy to implement. Our simulation results have confirm that even with low densities, forbidden substructure based wormhole detection algorithms have sound performance in both 2D and 3D.

Acknowledgements

This work is supported by the National Key R&D Program of China under grant 2018YFB100471, the National Natural Science Foundation of China (NSFC) under grants 61702298, 61632013, 61822205, and 61632020.

References

[1] J.I. Shiyu, T. Chen, S. Zhong, Wormhole attack detection algorithms in wireless network coding systems, IEEE Trans. Mob. Comput. 14 (3) (2015) 660–674.

[2] R. Maheshwari, J. Gao, S.R. Das, Detecting wormhole attacks in wireless networks using connectivity information, IEEE Int. Conf. Comput. Commun. (2007) 107–115.

[3] L. Qian, N. Song, X. Li, Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach, J. Netw. Comput. Appl. 30 (1) (2007) 308–330.

[4] R. Poovendran, L. Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks, Wireless Netw. 13 (1) (2007) 27–59.

[5] I. Khalil, S. Bagchi, N.B. Shroff, Liteworp: a lightweight countermeasure for the wormhole attack in multihop wireless networks, in: International Conference on Dependable Systems and Networks, 2005, pp. 612–621.

[6] X. Ban, R. Sarkar, J. Gao, Local connectivity tests to identify wormholes in wireless networks, in: Proceedings of the 12th ACM Interational Symposium on Mobile Ad Hoc Networking and Computing, ACM, 2011 13.

[7] I. Khalil, S. Bagchi, N.B. Shroff, Mobiworp: mitigation of the wormhole attack in mobile multihop wireless networks, Ad Hoc Netw. 6 (3) (2008) 344–362.

[8] Y.C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in: IEEE International Conference on Computer Communications, 3, 2003, pp. 1976–1986.

[9] L. Buttyán, L. Dóra, I. Vajda, Statistical wormhole detection in sensor networks., in: European Workshop on Security and Privacy in Ad-hoc and Sensor Networks, 2005, pp. 128–141.

[10] D. Dong, M. Li, Y. Liu, X.Y. Li, X. Liao, Topological detection on wormholes in wireless ad hoc and sensor networks, IEEE/ACM Trans. Netw. 19 (6) (2009) 1787–1796.

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

[12] Y. Ren, M.C. Chuah, J. Yang, Y. Chen, Detecting wormhole attacks in delay tolerant networks, IEEE Wireless Commun. 17 (5) (2010) 36–42.

[13] R. GarcÃapelayo, Distribution of distance in the spheroid, J. Phys. A Gen. Phys. 38 (16) (2005) 3475.

[14] B.N. Clark, C.J.C.S. Johnson, Unit disk graphs, Discrete. Math. (1–3) (1990) 165–177.

[15] D. Kim, Z. Zhang, X. Li, W. Wang, W. Wu, D.Z. Du, A better approximation algorithm for computing connected dominating sets in unit ball graphs, IEEE Trans. Mob. Comput. 9 (8) (2010) 1108–1118.

[16] I.F. Akyildiz, D. Pompili, T. Melodia, Underwater acoustic sensor networks: research challenges, Ad Hoc Netw. 3 (3) (2005) 257–279.

[17] H. Breu, D.G. Kirkpatrick, Unit disk graph recognition is NP-hard, Comput. Geom. 9 (1–2) (1998) 3–24.

[18] S. Bai, X. Che, X. Bai, X. Wei, Maximal independent sets in heterogeneous wireless ad hoc networks, IEEE Trans. Mob. Comput. 15 (8) (2016) 2023–2033.

[19] T. Tuuminen, Upper bound of density for packing of equal circles in special domains in the plane, Periodica Polytechnica Civil Eng. 44 (1) (2000) 13–32.

[20] Wikipedia, Circle packing in a circle, 2018, https://en.wikipedia.org/wiki/Circle_packing_in_a_circle.

[21] M.R. Garey, R.L. Graham, D.S. Johnson, Some np-complete geometric problems, in: ACM Symposium on Theory of Computing, 1976, pp. 10–22.

[22] M.R. Garey, D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman, 1986.

[23] J. Radhakrishnan, Greed is good: approximating independent sets in sparse and bounded-degree graphs, in: ACM Symposium on Theory of Computing, 1994, pp. 439–448.

[24] D. Zhang, J.P. Sterbenz, Robustness analysis and enhancement of MANETs using human mobility traces, J. Netw. Syst. Manag. 24 (3) (2016) 653–680.

[25] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, J. Jetcheva, A performance comparison of multi-hop wireless ad hoc network routing protocols, in: Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM, 1998, pp. 85–97.

[26] P. Juang, H. Oki, Y. Wang, M. Martonosi, L.S. Peh, D. Rubenstein, Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with Zebranet, ACM SIGARCH Comput. Archit. News 30 (5) (2002) 96–107.

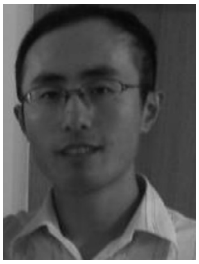
[27] M. Conti, R.D. Pietro, L. Mancini, A. Mei, Distributed detection of clone attacks in wireless sensor networks, IEEE Trans. Dependable Secure Comput. 8 (5) (2011) 685–698.

[28] Z. Zheng, A. Liu, L.X. Cai, Z. Chen, X.S. Shen, Energy and memory efficient clone detection in wireless sensor networks, IEEE Trans. Mob. Comput. 15 (5) (2016) 1130–1143.

[29] W. Wu, H. Du, X. Jia, Y. Li, C.H. Huang, Minimum connected dominating sets and maximal independent sets in unit disk graphs, Theor. Comput. Sci. 352 (1) (2006) 1–7.

Sen Bai received the B.S. degree from the School of Software Engineering, Huazhong University of Science and Technology, China, in 2008. He received the M.S. degree from Department of Computer Science, Jilin University, China, in 2013, where he received the Ph.D. degree in 2016. He holds a Post-doctoral position with the School of Software, Tsinghua University, under the supervision of Prof. Y. Liu. His research of interests are in the area of wireless ad hoc networks and intelligent transportation system.

Yunhao Liu received the B.S. degree from the Automation Department, Tsinghua University, and the M.A. degree from Beijing Foreign Studies University, China. He received the M.S. and Ph.D. degrees from Computer Science and Engineering, Michigan State University. He is now the ChangJiang professor at Tsinghua University. His research interests include sensor network and IoT, localization, RFID, distributed systems, and cloud computing. He is fellow of the ACM and IEEE.



Zhenhua Li received the B.Sc. and M.Sc. degrees from Nanjing University in 2005 and 2008, and the Ph.D. degree from Peking University in 2013, all in computer science and technology. He is an assistant professor in the School of Software, Tsinghua University. His research areas mainly consist of mobile Internet, cloud computing/storage, and content distribution. He is a member of the IEEE.

Xin Bai received the BS degree from the Department of Mathematics, Shanghai Jiao Tong University, China, in 2008. He received the MS degree from Department of Computer Science, Jilin University, China, in 2013, where he received the PhD degree in 2018. He is currently working in Huawei Technologies Co. Ltd.