Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach

L. Lazos¹, R. Poovendran¹, C. Meadows², P. Syverson², L. W. Chang²
¹University of Washington, Seattle, Washington, ²Naval Research Laboratory, Washington, DC
Email: {lazos, radha}@ee.washington.edu, {meadows, syverson, lchang}@itd.nrl.navy.mil

Abstract—We study the problem of characterizing the wormhole attack, an attack that can be mounted on a wide range of wireless network protocols without compromising any cryptographic quantity or network node. Making use of geometric random graphs induced by the communication range constraint of the nodes, we present the necessary and sufficient conditions for detecting and defending against wormholes. Using our theory, we also present a defense mechanism based on local broadcast keys. We believe our work is the first one to present analytical calculation of the probabilities of detection. We also present simulation results to illustrate our theory.

Index Terms—wormhole, security, vulnerability, ad hoc networks, geometric random graph.

I. INTRODUCTION

A wireless ad hoc network may be deployed in hostile environments, where network nodes operate un-tethered. In addition, the wireless medium exposes any message transmission to anyone located within the communication range. In this paper we investigate a specific type of emerging security threat known as the wormhole attack [1], [2]. In a wormhole attack an adversary records information at an origin point, tunnels it (via a faster or direct link) to a destination point more than one-hop away, and retransmits the information in the neighborhood of the destination. Since a wormhole attack can be launched without compromising any node, or the integrity and authenticity of the communication, the success of the attack is independent of the strength of the cryptographic method that protects the communication. Hence, a wormhole attack is implemented with few resources and is difficult to detect.

Several approaches have been presented for defending against the wormhole attack [1]–[3]. The solutions proposed attempt to bound the distance that any message can travel using time-based methods [1], [3], cryptography [2], or exploiting location information [1]. Time-based methods either rely on tight synchronization between the network nodes [1], or on measuring the time of flight of a challenge-response [3] using clocks with nanosecond accuracy. Location-based methods also require loose synchronization between nodes [1]. In [2], network nodes use cluster keys to broadcast to their immediate neighbors. However, the authors of [2] noted their system is vulnerable to wormholes during the key establishment phase, due to lack of any verification mechanism. On the other hand, we present a solution that utilizes a combination of location information and cryptography to prevent the wormhole attack. We list our contributions next.

Our contributions: We present a graph theoretic model for characterizing the wormhole attack and derive the necessary and sufficient conditions for any candidate solution to prevent wormholes. Using our theory, we then propose a Local Broadcast Key (LBK) based method to secure an ad hoc network from wormhole attacks. In doing so, we show that LBK solution satisfies the necessary graph theoretic condition. We also present a decentralized realization for LBK establishment, and provide an analytical evaluation of the security level achieved by our scheme based on spatial statistics theory.

Unlike in [1], [3], our solution does not require time synchronization, or highly accurate clocks, and only a small fraction of nodes need to know their location. Our approach has low overhead in computation and communication, suitable for wireless sensor networks.

The paper is organized as follows: The Section II describes the wormhole problem, and its graph theoretic representation. In Section III, we state our network model assumptions. Section IV shows how LBKs defend against wormholes and the presents a mechanism to establish them. In Section V, we describe how to secure LBK establishment mechanism from wormholes. In Section VI, we present the performance evaluation, and Section VII presents our conclusions.

II. PROBLEM STATEMENT

A. Description of wormhole

To launch a wormhole attack, an adversary establishes a direct link referred as wormhole link between two points in the network. A direct link can be established via a wireline, a long-range wireless transmission, or an optical link. Once the wormhole link is operational, the adversary eavesdrop messages at one end, referred as the origin point, tunnels them through the wormhole link and replays them in a timely fashion at the other end, referred as the destination point.

In the wormhole model, it is assumed that the adversary does not compromise the integrity and authenticity of the communication, and any cryptographic quantity remains secret.
Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach

1. REPORT DATE
2. REPORT TYPE
3. DATES COVERED
2005
3a. CONTRACT NUMBER
3b. GRANT NUMBER
3c. PROGRAM ELEMENT NUMBER
3d. PROJECT NUMBER
3e. TASK NUMBER
3f. WORK UNIT NUMBER
00-00-2005 to 00-00-2005

4. TITLE AND SUBTITLE
Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach

5. AUTHOR(S)

6. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Washington, Department of Electrical Engineering, Seattle, WA, 98195

7. PERFORMING ORGANIZATION REPORT NUMBER

8. SPONSOR/MONITOR'S NAME(S) AND ADDRESS(ES)

9. SPONSOR/MONITOR'S ACRONYM(S)

10. SPONSOR/MONITOR'S REPORT NUMBER(S)

11. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

12. SUPPLEMENTARY NOTES
The original document contains color images.

13. ABSTRACT

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:
   a. REPORT
      unclassified
   b. ABSTRACT
      unclassified
   c. THIS PAGE
      unclassified

17. LIMITATION OF ABSTRACT

18. NUMBER OF PAGES
   7

19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
If an adversary had access to cryptographic keys, it could generate and forge any authentic message, and inject it back into the network with no assistance from wormholes.

### B. Wormhole threat against network protocols

Various wormhole attack scenarios disrupting network protocols and applications are available from [1], [4]. We now illustrate how a wormhole attack can disrupt the distance vector based ad hoc routing protocols such as DSDV [5] or ADV [6].

Figure 1 presents an ad hoc network of 13 nodes and a wormhole link between nodes $s_9$ and $s_2$. If the routing table of node $s_9$ is tunneled through the wormhole link, node $s_2$ will hear the broadcast and assume that node $s_9$ is a one-hop neighbor. Node $s_2$ will update and broadcast its routing table entries for one-hop neighbor node $s_9$, and nodes $\{s_8, s_{10}, s_{11}, s_{12}\}$ that are now reachable via two hops. Similarly, other neighbors of $s_2$ will adjust their own routing tables. Note that nodes $\{s_1, s_3, s_4, s_5, s_7\}$ will now route via $s_2$ to reach any of the nodes $\{s_9, s_{10}, s_{11}, s_{12}\}$. Hence, with minimal resources, an attacker can redirect and observe a large amount of traffic as desired. Furthermore, by simply switching the wormhole link on and off, the attacker can trigger a route oscillation within the network, thus leading to a denial-of-service (DoS) attack.

From these examples, we note that a wormhole in essence creates a communication link between an origin and a destination point that could not exist with the use of the regular communication channel. Hence, a wormhole modifies the connectivity matrix of the network and can be described by a graph abstraction of the ad hoc network as described next.

### C. A Graph theoretic formulation.

Consider an ad hoc network randomly deployed with any node $i$ having a communication range $r$. Such a network can be modeled as a geometric random graph [7], defined as follows:

**Geometric Random Graph:** Given a finite set of vertices $V \subseteq \mathbb{R}^d$ ($d = 2$ for 2-dimensional space), we denote by $G(V, r)$ the undirected graph with vertex set $V$ of randomly deployed nodes, and with undirected edges connecting pairs of vertices $(i, j)$ with $\|i - j\| \leq r$, where $\| \cdot \|$ is some norm on $\mathbb{R}^d$ [7]. The entries of the edge, or connectivity matrix, denoted by $e$, are given by:

$$ e(i, j) = \begin{cases} 1, & \text{if } \|i - j\| \leq r \\ 0, & \text{if } \|i - j\| > r \end{cases} $$ (1)

The existence of wormhole links violates the geometric graph model, by allowing links longer than $r$, thus transforming the initial geometric graph $G(V, r)$ into a logical connectivity graph $\tilde{G}(V, E_\tilde{G})$, where arbitrary connections can be established. Hence, a non-trivial wormhole will always increase the entries of the connectivity matrix of $G(V, r)$.

A candidate solution preventing the wormhole attack should reconstruct the original geometric random graph $G(V, r)$, or by imposing a less strict requirement, should transform the logical graph $G(V, E_\tilde{G})$ to a logical graph $G'(V, E_{G'})$, in which, for any link between a pair of nodes $i, j$, condition 1 is always satisfied. We formalize these ideas in theorem 1.

**Theorem 1:** Given a geometric random graph $G(V, r)$ defined as in (1), and an arbitrary logical graph $\tilde{G}(V, E_\tilde{G})$, a transformation $S : G \times \tilde{G} \to G'$ of $\tilde{G}(V, E_\tilde{G})$ into a logical graph $G'(V, E_{G'})$ is a solution to the wormhole problem iff the set of edges of $G'$ is a subset of the set of edges of the $G(V, r)$, i.e. $E_{G'} \subseteq E_G$.

**Proof:** Assume that $G' = S(G, \tilde{G})$ prevents the wormhole attack. Let $C_X$ denote the connectivity matrix of graph $X$. If $E_{G'} \not\subseteq E_G$, there exist a pair of nodes $(i, j)$ for which: $C_{G'}(i, j) = 0$ and $C_{\tilde{G}}(i, j) = 1$. For such node pairs, $e(i, j) = 1$, with $\|i - j\| > r$, violating the communication range constraint. Hence, in order for $S(G, \tilde{G})$ to prevent the wormhole attack, it follows that: $E_{G'} \subseteq E_G$.

The converse follows immediately. If $E_{G'} \subseteq E_G$, then $C_{G'}(i, j) \leq C_{\tilde{G}}(i, j), \forall i, j \in V$. Hence, there is no edge $e'(i, j) \in E_{G'}$ such that $e'(i, j) = 1$, $\|i - j\| > r$, and hence, the graph $G'$ is void of any wormhole.

A trivial graph $G'$ with no links ($E_{G'} = \emptyset$) satisfies the conditions of the theorem 1. However, to ensure communication between all network nodes, we seek solutions that construct a connected graph.

We also note that the transformation $G' = S(G, \tilde{G})$ requires the knowledge of the geometric random graph $G(V, r)$, defined by the location of the vertices, and the communication range $r$. When nodes do not have a global view of the network (know the location of other nodes), to verify theorem 1, we must indirectly construct a connected subgraph of the geometric random graph $G(V, r)$. Before we present our solution on constructing such subgraph, we describe the needed network model assumptions.

### III. Network Model Assumptions

**Network setup:** We assume that the network nodes are randomly deployed within a specific region. We also assume that a small fraction of network nodes, called *Guards* is assigned special network operations. Density of the regular network nodes is assumed to be $\rho_s$, and the density of the guards is assumed to be $\rho_g$, with $\rho_s \gg \rho_g$. We assume that all nodes utilize omnidirectional antennas. Communication range of regular nodes is $r$, while that of guards is $R$ with $R > r$.

**Resource constraints:** We assume that guards have access to location information through GPS [8] or some other localization method, though regular node may have no location information.
We also assume that nodes rely on efficient symmetric cryptography for encryption/decryption, authentication and hashing. We also assume that nodes can be pre-loaded with keys.

**Statistical network model:** It can be shown [11] that the random deployment of the nodes and guards in an area $A$ can be modeled after a Spatial Homogeneous Poisson Point Process [11]. The random placement of the set $U$ of guards with a density $\rho_\gamma = \frac{|U|}{|A|} (|\cdot|)$ denotes the cardinality of a set) is equivalent to a sequence of events following a homogeneous Poisson point process of rate $\rho_\gamma$. The random deployment of a set $S$ of nodes with a density $\rho_s = \frac{|S|}{|A|}$, is equivalent to a random sampling of $A$ with rate $\rho_s$ [11].

Based on Spatial Statistics theory [11], if $GH_s$ denotes the set of guards heard by a node $s$, the probability that a node hears exactly $k$ guards is given by the Poisson distribution:

$$P(|GH_s| = k) = \frac{(\rho_\gamma \pi R^2)^k}{k!} e^{-\rho_\gamma \pi R^2} \tag{2}$$

Using the model in (2), we will analytically evaluate the performance of our algorithms.

**IV. LOCAL BROADCAST KEYS**

In this section, we first define LBKs and show that LBKs can be used to defend against wormhole. We then present details of a decentralized mechanism for establishing LBK, followed by a probabilistic analysis of the security of the LBK scheme.

**Definition:** For a node $i$, we define the neighborhood $N_i$ as: $N_i = \{ j : \|i-j\| \leq r \}$. Given a cryptographic key $K$, let $U_K$ denote the set of nodes that hold key $K$. We assign a unique key $K_i$ called LBK of $i$, to all $j \in N_i$ so that $U_{K_i} = N_i$ and $K_i \neq K_j, \forall i \neq j$. Hence, by definition, all one-hop neighbors of node $i$ possess the LBK of node $i$. We follow the convention that any message from node $i$ to $j$ is encrypted with $K_i$. Hence, a link between nodes $i, j$ exists if $i \in N_j$ or $j \in N_i$.

**Theorem 2:** Given $K_i, N_i, \forall i \in V$, where $V$ is the set of vertices defined by network nodes, and an arbitrary logical random graph $G(V, E_G)$, the edge matrix $E_G$, defined by:

$$e_G(i, j) = \begin{cases} 1, & \text{if } i \in U_{K_j} \cup j \in U_{K_i} \\ 0, & \text{if Else} \end{cases} \tag{3}$$

yields the desired wormhole-free graph $G'(V, E_{G'})$ such that $E_{G'} \subseteq E_G$, where $G(V, r)$ is the geometric random graph defined in (1).

**Proof:** By the definition of $E_G$, there exists a link $e_G(i, j)$ if and only if the two nodes hold at least one LBK. But, according to the definition of LBK, a node $i \in U_{K_j}$, iff $i \in N_j$, which in turn implies that $i, j$ satisfy (1), which defines the links of the geometric random graph $G(V, r)$. Hence, $e_G(i, j) = 1$, iff $\|i-j\| \leq r$. Hence, $E_G = E_G$ and therefore, $G' \equiv G$. According to theorem 1, if a transformation $S(G, G')$ results in a graph $G'(V, E_{G'})$ such that $E_{G'} \subseteq E_G$, then $G'$ is a wormhole-free graph.

Note that given LBKs for all nodes, wormholes can be eliminated without ever having to know the location of any node. However, the challenge is to establish LBKs in the presence of wormhole links and no central authority.

**A. Decentralized establishment of local broadcast keys**

We present a three-step algorithm for LBK establishment. In the first step, the guards distribute fractional keys $FK_i$ to nodes via broadcasting. In step 2, every node broadcasts the Ids of the fractional keys that it holds. If two nodes share more than a threshold $th$ number of fractional keys, they use all common fractional keys to generate a pairwise key. In step 3, every node uses the pairwise keys to securely unicast a local broadcast key to each neighbor. We first present the cryptographic mechanisms of our LBK scheme.

1) **Cryptographic Mechanisms**

**Encryption:** To protect the distribution of the fractional keys, all transmissions from the guards are encrypted with a globally shared symmetric key $K_0$, pre-loaded before deployment. In addition, every node shares a symmetric pairwise key $K_{i,g}$ with every guard $g_i$, also pre-loaded. In order to save storage space at the guard side, the pairwise key $K_{i,g}$ is derived using a pseudo-random function $\pi_R$ and the unique ID of the guard $g_i$, $K_{i,g} = \pi_R(g_i | Id_i)$. Hence, given an ID, a guard can compute its pairwise key with the node Id whenever needed.

**Guard Id authentication:** To authenticate the source of the fractional keys we use efficient one-way hash chains [9]. Each guard $g_i$ has a unique password $PW_i$, blinded with the use of a collision-resistant hash function such as SHA1 [12]. Due to the collision resistance property, it is computationally infeasible for an attacker to find $PW_i$, such that $H(PW_i) = H(H(PW_i))$, $PW_i \neq PW_i$. The hash chain is generated as follows:

$$H^0 = PW_i, \ H^i = H(H^{i-1}) = 1, \cdots , n$$

with $n$ being a large number and $H^0$ never revealed to any node. Due to the one-way property it is also infeasible to compute any values of the hash chain that have not been published by a guard. Each node is pre-loaded with a table containing the ID of each guard and the corresponding hash value $H^m(PW_i)$. To reduce the storage needed at the guard side, guards use an efficient storage/computation method for hash chains of time/storage complexity $O(\log^2(n))$ [10].

2) **Steps of the key establishment scheme**

[Step 1:] Initially, every guard $g_i$ generates a random fractional key $FK_i$ and broadcasts it. The broadcast message also contains the coordinates $(X_i, Y_i)$ of the guard, the next unpublished value of the hash chain, $H^{n-m}(PW_i)$, and the hash chain index $m$ ($m$ also indicates how many beacons has each guard transmitted). The message format is:

$$\text{Guard } g_i : \{FK_i, ||(X_i, Y_i)||H^{n-m}(PW_i)||m\}_{K_0} \tag{4}$$

where $\{A||B\}_K$ denotes concatenation of $A, B$ and encryption with key $K$. Every node verifies that $H(H^{n-m}(PW_i)) = H^{n-m+1}(PW_i)$, for all received messages and stores the $FK_i$, the coordinates $(X_i, Y_i)$, the latest published hash value of the hash chain, $H^{n-m}(PW_i)$,
and the hash index \( m \).

**[Step 2]:** Once the nodes have collected the fractional keys from all the guards that they hear, they broadcast a message indicating the IDs of the fractional keys that they hold. If two neighbor nodes \( s_1, s_2 \) have in common fractional keys \( FK_1 \ldots FK_w \) with \( w \) above a threshold \( th \), they establish a pairwise key: \( K_{s_1, s_2} = H(FK_1 || FK_2 || \ldots || FK_w) \), where \( H \) is a collision-resistant hash function [9].

**[Step 3]:** After pairwise keys have been established with one-hop neighbors, every node generates a LBK \( K_i \) and unicasts it to every neighbor encrypted with the pairwise key \( K_{s_i, s_j} \). Each node stores its own broadcast key \( K_i \) used for encrypting its own messages, and also stores all broadcast keys of its one-hop neighbors in order to decrypt their broadcast messages.

In figure 2(a) the guards \( g_1 \sim g_5 \) distribute the fractional keys to nodes \( s_1 \sim s_7 \), encrypted with the global key \( K_0 \). In figure 2(b), we show the set of guards that each node hears. In figure 2(c), by setting the threshold value \( th = 3 \), node \( s_1 \) establishes a pairwise key with all its immediate neighbors. Node \( s_1 \) will distribute a local broadcast key \( K_{s_1} \) to all its immediate neighbors \( s_1 \sim s_5 \) using the pairwise keys established in step 2. In figure 3, we summarize our decentralized local broadcast key establishment scheme.

### Decentralized local broadcast key establishment scheme

\[
U = \{ \text{Set of guards} \}, \quad S = \{ \text{Set of nodes} \} \\
U : \text{Broadcast } \{ FK_i || V \}_{i=0}^{m} | \text{[Set of broadcast keys]} | K_0 \\
S : \text{Verify } H(H^n + F(PW_i)) = H^n - k + 1 \forall i \in GH_s \\
S : \text{Broadcast } ID_{s_i} = \{ ID_1 || ID_2 || \ldots || ID_w \}, |GH_s| = w \\
\text{for all } s_i \in S \\
\text{for all } ID_{s_i} \text{ heard by } s_i \\
\text{if } |ID_{s_i}||ID_{s_j}| > th, \quad s_j \in N_{s_i} \rightarrow K_{s_i, s_j} = H(FK_1 || FK_2 || \ldots || FK_w) \\
N_{s_i} = N_{s_i} \cup \{ s_j \} \end{cases}
\]

end for

\[
\text{for all } s_j \in S \\
\quad s_i \rightarrow s_j : \{ K_{s_i, s_j} \} \quad \text{end for}
\]

**Fig. 3.** The decentralized local broadcast key establishment scheme.

![Fig. 2.](image) (a) Guards \( g_1 \sim g_5 \) broadcast fractional keys \( K_1 \sim K_5 \) encrypted with the global broadcast key \( K_0 \). (b) Nodes announce the IDs of the fractional keys that they hold. (c) Neighbor nodes that have in common at least three fractional keys \((th = 3)\) establish a pairwise key.

![Fig. 4.](image) (a) All guards located in the shaded area \( A_s \) are heard to both nodes \( s_1, s_2 \). (b) \( P_{key} \) for a variable threshold value equal to \( th = |GH_s| - 3 \).

### B. Setting the key establishment threshold

Since nodes and guards will be randomly deployed within the network region, specific number of guards heard by nodes may vary. Hence, each node needs to locally decide the threshold \( th \) based on the number of guards that it hears.

Consider figure 4(a), and assume that a node \( s_1 \) can hear \( |GH_{s_1}| \) guards. The probability \( P_{key} \) that \( s_1, s_2 \) hear at least \( th \) common guards given that \( |GH_{s_1}| \) guards are heard by \( s_1 \) is equal to the probability that at least \( th \) guards are located within the shaded area \( A_c \), given that \( |GH_{s_1}| \) of them are located within the communication area of \( A_{s_1} \) of \( s_1 \). Due to the random guard deployment, if \( |GH_{s_1}| \) guards are located within a specific region, those guards are uniformly distributed [11]. Hence, the probability for one guard to be within \( A_c \) is \( p_g = \frac{\pi R^2}{\pi R^2} \). The probability that more than \( th \) guards are deployed within \( A_c \), given that a total of \( |GH_{s_1}| \) are deployed within \( \pi R^2 \) is:

\[
P_{key} = P(|GH_{A_c}| \geq th \mid |GH_{s_1}| = k) \\
= \sum_{i=0}^{k-th} \binom{k}{th+i} p_g^{th+i} (1 - p_g)^{k-th-i} \\
= \sum_{i=0}^{k-th} \binom{k}{th+i} \frac{A_c}{\pi R^2}^{th+i} (1 - \frac{A_c}{\pi R^2})^{k-th-i}
\]

(5)

where \( A_c \) can be computed from figure 4(a) by:

\[
\phi = \cos^{-1} \left( \frac{l}{2R} \right) \quad A_c = 2R^2 \phi - Rl \sin \phi
\]

(6)

with \( l = ||s_1 - s_2|| \). Using (5), (6), each node can determine its threshold \( th \). In figure 4(b), we present \( P_{key} \) for different
values of guards heard $|GH_{s_1}|$ and distances $|s_1 - s_2|$, for $th = |GH_{s_1}| - 3$.

V. SECURING THE BROADCAST OF FRACTIONAL KEYS

Though once established LBKs prevent wormholes (information encrypted at a neighborhood $N_i$ with an LBK $K_i$ cannot be decrypted outside $N_i$), an adversary can mount wormhole during the distribution of the fractional keys. We now provide mechanism to secure the fractional key distribution.

A. Wormhole attack against the fractional key distribution

Consider figure 5, where an adversary establishes a bidirectional wormhole link between nodes $s_1$, $s_2$, with $s_1$, $s_2$ being several hops away. In step 1 of the local broadcast key establishment scheme, guards broadcast their fractional keys. The adversary records all messages heard by $s_1$, $s_2$ and replays the messages heard to $s_1$ in the vicinity of $s_2$, and messages heard by $s_2$ in the vicinity of $s_1$. After the replay, $s_1$, $s_2$ have a common set of fractional keys $GH_{s_1} \cup GH_{s_2}$.

B. Detection of the wormhole attack

We now show how a node can detect a wormhole attack during the fractional key distribution using two properties:

Single guard property: Reception of multiple copies of an identical message from the same guard is due to replay or multipath effects.

Proof: Since guards include a different hash value from the hash chain on every message they transmit, if a node receives an identical message more than one times, it can only be because, (a) a malicious entity replays the message or (b) there are multipath effects. If we treat multipath effects as a replay attack, then any node receiving the same transmission multiple times, assumes it is under a replay attack.

In figure 6(a), $A_s$ denotes the area where guards heard to node $s$ are located (circle of radius $R$ centered at $s$), $A_c$ denotes the area where guards heard at the origin point of the attack are located (circle of radius $R$ centered at $O$) and $A_o$ denotes the common area $A_c = A_s \cap A_o$. An adversary that records guards’ transmissions heard at point $O$ and replays them to node $s$ can be detected due to the single guard property with a probability $P(SG)$ equal to the probability that at least one guard lies within $A_s$.

$$P(SG) = P(|GH_{A_s}| \geq 1) = 1 - e^{-\rho_s A_s}$$

In figure 6(b), we show the detection probability $P(SG)$ for guard densities $\rho_g$, for distances $0 \leq |s - O| \leq 3R$, normalized over $R$. We observe that if $|s - O| \geq 2R$, the single guard property cannot detect a wormhole attack. We make use of the following property to identify wormholes when $|s - O| \geq 2R$.

Communication range constraint property: A node $s$ cannot hear two guards $g_i$, $g_j \in GH_s$, that are more than $2R$ apart, i.e. $|g_i - g_j| \leq 2R$, $\forall i, j$, $i \neq j$.

Proof: Any guard $g_i \in GH_s$ heard by node $s$, has to lie within a circle of radius $R$, centered at the node $s$, $|g_i - s| \leq R, \forall i \in GH_s$. Hence, there cannot be two guards within a circle of radius $R$, that are more than $2R$ apart.

$$|g_i - g_j| \leq |g_i - s| + |s - g_j| \leq R + R = 2R$$

We now compute the detection probability $P(CR)$ based on the communication range constraint property. Consider figure 6(c) where any two guards within $A_i$, $A_o$ have a distance larger that $2R$ the attack is detected. Though $P(CR)$ is not easily computed analytically, we can extract a lower bound on $P(CR)$ as follows. In figure 6(c), the vertical lines defining shaded areas $A_i$, $A_j$, are perpendicular to the line connecting $s$, $O$, and have a separation $2R$. If there is at least one guard in the shaded area $A_i$ and at least one guard in the shaded area $A_j$, then $|g_i - g_j| > 2R$ and the attack is detected. Note that this event does not include all possible cases for which $|g_i - g_j| > 2R$, and hence it yields a lower bound.

$$P(CR) = P(|g_i - g_j| > 2R, g_i, g_j \in GH_s)$$

$$\geq P(CR | \bigcap_{i, j} |GH_{A_i}| > 0 \cap |GH_{A_j}| > 0)$$

$$\geq P(\bigcap_{i, j} |GH_{A_i}| > 0 \cap |GH_{A_j}| > 0)$$

$$\geq P(\bigcap_{i, j} |GH_{A_i}| > 0 \cap |GH_{A_j}| > 0)$$

$$= (1 - e^{-\rho_s A_i})(1 - e^{-\rho_s A_j})$$

where (9) follows from the fact that the probability of the intersection of two events is always less or equal to the probability of one of the events, (10) follows from the definition of the conditional probability, (11) follows from the fact that $|GH_{A_i}| > 0 \cap |GH_{A_j}| > 0$, we always have a communication range constraint violation $(P(CR | \bigcap_{i, j} |GH_{A_i}| > 0 \cap |GH_{A_j}| > 0) = 1)$, and $(12)$ follows from $A_i$, $A_j$ being disjoiint areas.

We can show that the lower bound on $P(CR)$ is maximized when $A_i = A_j$, but the proof is omitted due to space limitations. In figure 6(d), we show the lower bound on $P(CR)$, by setting $A_i = \max_i \{ A_i \}$ such that $A_i = A_j$. Note that for values $|s - O| > R$, $P(CR)$ is very close to unity for any value of $\rho_g$. The lower bound $P(CR)$ increases with the increase of $|s - O|$ and attains its maximum value for $|s - O| = 4R$ when $A_i = A_j = \pi R^2$. For values $|s - O| > 4R$ the lower bound on $P(CR)$ is equal to the case of $|s - O| = 4R$. 
Detection probability of a wormhole attack: By combining the two previously presented detection mechanisms we can derive a lower bound on the probability of wormhole detection $P_{\text{det}}$ during the broadcast of the fractional keys. By setting $A_i = A_j$ and maximizing $A_i$ regardless of the distance $\|s-O\|$, the areas $A_i$, $A_j$, $A_s$ do not overlap as shown in figure 8(a).

Hence, the events of a guard being located at any of these areas are independent and we can derive a lower bound on $P_{\text{det}}$:

$$
P_{\text{det}} = P(SG \cup CR) = P(SG) + P(CR) (1 - P(SG)) \\
\geq (1 - e^{-\rho g A_i}) + (1 - e^{-\rho g A_j}) e^{-\rho g A_s} \tag{13}
$$

The quantity in (13) is a lower bound on $P_{\text{det}}$ since we used the lower bound on $P(CR)$. In figure 8(b), we show the lower bound on $P_{\text{det}}$ for $R \in [0,4R]$. Note that the lowest detection probability is $P_{\text{det}} \geq 99.48\%$, attained at $\rho g = 0.01$. From figure 8(b), we observe that a wormhole attack during the distribution of the fractional keys is detected with a probability very close to unity, independent of the distance $\|s-O\|$.

C. Key establishment in the presence of wormholes

Although a wormhole can be detected using the two detection mechanisms, a node under attack cannot distinguish the valid subset of guards from the replayed ones. We now describe the Closest Guard Algorithm (CGA) to resolve the guard ambiguity.

CGA – The node $s$ broadcasts a nonce $\eta$ along with its Id and waits for the first authentic reply from a guard $g_i$. All guards that hear nonce $\eta$, reply with a message containing their coordinates, the next hash value of their hash chain and the nonce $\eta$. The message transmitted from each guard is encrypted with the pairwise key $K^\eta_{i,s}$ only known to $s$, $g_i$. The node identifies the guard $g'_i$ whose reply arrives first as the closest guard to $s$. Then using the communication range constraint property, it identifies the set $GH'_s$ as all the guards that are not more than $2R$ away from $g'_i$ and uses the fractional keys received from $GH'_s$ to establish pairwise keys with its immediate neighbors.

To execute CGA, a node must be able to communicate bi-directionally with at least one guard. The probability $P_{s\rightarrow g}$ of a node having a bi-directional link is: $P_{s\rightarrow g} = 1 - e^{-\rho g \pi r^2}$. From $P_{s\rightarrow g}$, we can compute the probability $P_{bd}$ that all nodes can bi-directionally communicate with at least one guard: $P_{bd}$ =

VI. PERFORMANCE EVALUATION

Simulation setup: We generated random network topologies confined in a square area of size $A = 10,000$. For each network topology we randomly placed, (a) 5,000 nodes within $A$, with a communication range $r = 4$, (b) guards with variable density $\rho g$ and communication range $R$. To ensure statistical validity, we repeated each experiment for 1,000 networks and averaged the results. Note that to avoid border effects we considered toroidal distance instead of regular Euclidean distance [11].

Key establishment with one-hop neighbors: In our first experiment we evaluated the percentage of one-hop (immediate) neighbors $p_{\text{immed}}$ that each node is able to establish a local broadcast key with. In figure 7(a), we present $p_{\text{immed}}$ vs. $GH_s - \theta$ for variable guard density $\rho g$. Note that we preferred
VII. Conclusion

We presented a graph theoretic approach characterizing recently reported [1] wormhole attacks on wireless ad hoc networks. We derived the necessary and sufficient conditions for any transformation to remove wormholes, and showed that any candidate solution preventing a wormhole attack must produce a connected subgraph of the geometric graph model of the network. We also proposed a cryptography-based solution relying on local broadcast keys and provided a distributed mechanism for establishing them in randomly deployed networks. We analytically determined the level of security achieved by our scheme based on spatial statistics theory. We showed that the appropriate choice of network parameters eliminates wormhole links with a probability close to unity and verified the validity of our results via simulations. It is our claim that in the absence of location or distance bounding, we must use probabilistic techniques for dealing with wormholes.

REFERENCES