Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 763187, 12 pages
doi:10.1155/2012/763187

Research Article

Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques

Mariano García-Otero and Adrián Población-Hernández

Departmento de Señales, Sistemas y Radiocomunicaciones, ETSI de Telecomunicación, Universidad Politécnica de Madrid, Avenida Complutense 30, 28040 Madrid, Spain

Correspondence should be addressed to Mariano García-Otero, mariano@gaps.ssr.upm.es

Received 14 July 2012; Revised 27 September 2012; Accepted 27 September 2012

Academic Editor: An Liu

If a wireless sensor network (WSN) is deployed in a hostile environment, the intrinsic limitations of the nodes lead to many security issues. In this paper, we address a particular attack to the location and neighbor discovery protocols, carried out by two colluding nodes that set a wormhole to try to deceive an isolated remote WSN node into believing that it is a neighbor of a set of local nodes. To counteract such threat, we present a framework generically called detection of wormhole attacks using range-free methods (DWARF) under which we derive two specific wormhole detection schemes: the first approach, DWARFLoc, performs jointly the detection and localization procedures employing range-free techniques, while the other, DWARFTest, uses a range-free method to check the validity of the estimated position of a node once the location discovery protocol is finished. Simulations show that both strategies are effective in detecting wormhole attacks, and their performances are compared with that of a conventional likelihood ratio test (LRT).

1. Introduction

Wireless sensor networks (WSNs) are composed of a potentially large number of low-cost and resource-constrained devices which are often distributed over a wide area. Thus, if a WSN is deployed in an unfriendly environment, providing security to the involved network protocols is a challenging task that usually requires the use of different combined strategies [1].

A protocol that deserves special attention from a security point of view is neighbor discovery (ND). This is because one of the most basic requirements in a WSN is the ability of every node to reliably determine which of the other nodes are within its radio range so that it can establish single-hop links with them. Trustworthy ND is a cornerstone for securing higher-level network protocols and system functionalities, such as physical and network access control, data routing, and node localization [2].

In a hostile environment, a WSN can be compromised by different threats, but the so-called wormhole or relay attack lies among the most devastating [3]. A wormhole is a high-speed direct communication link between two malicious nodes that act in collusion by capturing network packets on one end, sending them through the wormhole and replaying them at the other end. Thus, to launch a wormhole attack, an adversary does not need to infect any network node or break any cryptographic system, making it a quite severe threat to WSNs.

Wormholes completely distort the network topology, making distant nodes to appear as local for a given node looking for its neighbors. As a side effect of a failed ND due to a wormhole, most location discovery (LD) protocols will also be compromised; this is because the wormhole severely distorts all the measurements related to the relative positions of the nodes. However, in some cases, the high sensitivity of

LD protocols to wormholes can be turned into an advantage, because the localization process can be suitably modified to detect the presence of an attack.

In this paper we address this approach for the detection of wormholes. Specifically, we propose a general framework called detection of wormhole attacks using range-free methods (DWARF) that has two modes of operation: the first one (DWARFLoc) performs the detection of a wormhole simultaneously with the localization procedure, while the second one (DWARFTest) is a postlocalization detector that tries to validate the node position after this latter is obtained. The principles of DWARF are rooted in the exploitation of the ideas underlying the operation of a range-free localization method, namely, the so-called "sensor localization with Ring Overlapping based on Comparison of Received Signal Strength Indicator" (ROCRSSI) algorithm [4].

The main contributions of this paper are as follows.

(i) The formulation of a simplified attack model for which the detection of a wormhole can be rigorously formulated as a binary hypothesis testing problem.

(ii) The derivation of the likelihood ratio test (LRT) as the asymptotically optimal solution for the wormhole detection problem. However, the LRT requires a precise statistical model for the observations.

(iii) The derivation of DWARFLoc and DWARFTest as robust alternatives to the LRT, because they are not tied to any particular channel model.

(iv) The evaluation of the relative performances of both categories of tests (LRT and DWARF) through simulations.

The rest of the paper is organized as follows. Section 2 reviews related work concerning wormhole detection. Section 3 presents basic ideas about range-free localization and briefly describes the ROCRSSI algorithm. Section 4 defines the particular attack to be counteracted. Section 5 formulates the wormhole detection problem under the framework of statistical hypothesis testing and derives the LRT. Section 6 presents the two wormhole detection strategies DWARFLoc and DWARFTest. Section 7 evaluates the performance of the different wormhole detection strategies through simulations. Finally, section 8 draws some conclusions.

2. Related Work

In recent years, the topic of secure ND has been extensively studied and a lot of different defensive measures against wormhole attacks are described in the related literature.

For instance, it is proposed in [3] the use of location and time stamps, that is, geographical and temporal "leashes", attached to network packets to detect wormhole attacks; therefore, this strategy assumes that all the nodes know their exact positions and are synchronized in time, which are probably unrealistic hypotheses if the network is under attack.

In [5], a wormhole detection algorithm for a multihop wireless network is presented, based on a search of forbidden substructures in the connectivity graph.

The authors of [6] present different preventive mechanisms against wormholes and propose an intruder detection system, LIDeA, in which every node analyzes their neighbors and collaborates to detect suspicious nodes using a voting strategy.

In [7], the authors introduce a graph-based and beaconless solution that detects wormholes visually by reconstructing the network topology using only inaccurate distances between the nodes; however, an irregular-shaped network or multiple wormholes may lead to an incorrect detection.

The cryptographic concept of "pairing" is introduced in [8]. The article describes a node-to-node neighborhood authentication protocol based on location-based keys (private keys of individual nodes that are bound to their identities and positions), to avoid malicious nodes to join the network.

Wu et al. [9] propose a localization scheme based on hop counts (DV-Hop) by labeling the neighboring nodes of beacon nodes according to different algorithms to detect wormhole attacks; nevertheless, the proposed scheme does not work well if the network has packet losses or the transmission ranges of all nodes are not identical.

Robust localization techniques were described in [10, 11], using the concept of "verifiable multilateration." Both are range-based approaches: while ROPE [10] provides secure localization and location verification using directional antennas and distance bounding, SPINE [11] estimates the distances between the nodes by measuring the time of flight of the radio signal. These solutions require either perfectly known directional antennas or specific transceivers capable of measuring the time of flight.

A secure range-free localization method called SeRLoc was proposed in [12], where the nodes are supposed to be equipped with static directional antennas with a fixed communication range, the nodes are localized by overlapping regions within communication range, and the wormholes are detected by checking the properties of message uniqueness and communication range violation. HiRLoc [13] is the evolution of SeRLoc and provides a high-resolution localization by adding two variables to the localization algorithm, the angle of rotation of the antennas, and the transmission power, increasing the complexity of the nodes.

Recently, ConSetLoc [14] proposes a robust range-free localization scheme based on evaluating the relationship between hops and distances and then applying convex constraints in geometry to reduce localization errors induced by wormholes.

For moving nodes, a secure ND protocol called MSDN [15] has been proposed, applying the notion of graph rigidity to aid moving network nodes in the verification of neighbors.

All the procedures for secure ND described above assume that the two colluding nodes forming a wormhole are located within the network deployment area. However, as we will see in Section 4, the particular threat we will address in this paper assumes that one of the wormhole nodes is situated out of the range of the WSN nodes but in the vicinity of an isolated node which is the target of the attack. So, this particular

wormhole attack to the LD and ND protocols cannot be detected by conventional techniques.

3. Range-Free Localization

Traditional localization techniques rely on providing network nodes with auxiliary devices capable of self-acquiring their coordinates in a geographical reference system, such as global positioning system (GPS) receivers. Such solutions, however, have severe drawbacks in terms of their cost and energy consumption and are unable to operate indoors. A much more flexible approach to LD is obtained if we assume that only a small number of network nodes are assumed to know their own locations (through GPS receivers or system configuration), while the other nodes are only able to measure their relative distances to other neighbor nodes and use these data to position themselves. Focusing on the physical layer (PHY) level, received signal strength (RSS) is a parameter readily available in most commercial sensor nodes, usually in a coarsely quantized form called RSS indicator (RSSI). RSS measurements can be used for localization, because they are related to the distances between nodes [16, 17]; however, as they strongly depend on the particular hardware used and also on often unpredictable environment conditions, in many cases they cannot be used to directly estimate distances. Therefore, in recent times several "range-free" alternatives to localization have been proposed; these methods use an indirect approach and provide localization without the need of accurate distance estimations.

We point here that there is some controversy regarding the expression "range-free" when applied to localization because, for some authors, this term only refers to techniques based on connectivity information, which can be interpreted as a binary quantization of RSS. We will, however, adopt a broader interpretation of "range-free" schemes as those that use RSS values but do not rely on the existence of any precise relationship between RSSs and distances, only assuming there is a loose link between these parameters [18]. We will also call these methods "nonparametric," as opposed to "parametric" or "range-based" approaches, which require a precise model relating RSS values to distances.

For instance, if we denote the Euclidean distance between two arbitrary network nodes at positions $\mathbf{x}$ and $\mathbf{y}$ as $d(\mathbf{x},\mathbf{y}) \equiv ||\mathbf{x}-\mathbf{y}||$ and the RSS (in dBm) measured at the receiver of node $\mathbf{y}$ for a signal transmitted by node $\mathbf{x}$ as $r(\mathbf{x},\mathbf{y})$, a common basic assumption in many range-free methods is the validity of a simple monotonicity constraint:

$$r(\mathbf{x},\mathbf{y}) > r(\mathbf{x},\mathbf{y}) \Longleftrightarrow d(\mathbf{x},\mathbf{y}) < d(\mathbf{x},\mathbf{y}),\ \forall \mathbf{x},\mathbf{y},\mathbf{z} \in \mathbb{R}^2. \tag{1}$$

Notice that because the transmitted power is assumed to be unknown, RSS measurements are not expected to be symmetric that is, $r(\mathbf{x},\mathbf{y}) \neq r(\mathbf{y},\mathbf{x})$. One of the most straightforward approaches to the solution of the problem of localizing a node based on the restriction (1) is given by the so-called ROCRSSI algorithm [4].

This range-free localization method assumes that there is a node trying to estimate its own unknown position $\mathbf{p}$, surrounded by N "anchor nodes" located at known positions $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N$. Every anchor node is continuously broadcasting beacon packets that include, along with its own location, the RSS values corresponding to beacon signals received from all the other anchor nodes in its vicinity. Therefore, for every anchor $\mathbf{a}_i$ $(i = 1, 2, \ldots, N)$ in the neighborhood of $\mathbf{p}$, we will assume that the following RSS values are available:

One anchor-to-node RSS: $r(\mathbf{a}_i, \mathbf{p})$,

$N-1$ anchor-to-anchor RSSs: $r(\mathbf{a}_i, \mathbf{a}_j)$, for all $i \neq j$.

Now, by applying the monotonicity constraint (1) to this set of RSS measurements, the localization algorithm obtains the tightest possible lower and upper bounds, $\rho_1^{(i)}$ and $\rho_2^{(i)}$, respectively, for the possible values of the distance between the ith anchor and the node to be located; this, in turn, translates to a restriction in the position of the node as a ring $R(\mathbf{a}_i, \rho_1^{(i)}, \rho_2^{(i)})$, centered around $\mathbf{a}_i$ and with inner and outer radii $\rho_1^{(i)}$ and $\rho_2^{(i)}$; respectively,

$$R\left(\mathbf{a}_i, \rho_1^{(i)}, \rho_2^{(i)}\right) = \left\{\mathbf{p} \in \mathbb{R}^2 : \rho_1^{(i)} < d(\mathbf{a}_i, \mathbf{p}) < \rho_2^{(i)}\right\}, \quad i = 1, 2, \ldots, N, \tag{2}$$

with $\rho_1^{(i)}$ and $\rho_2^{(i)}$ obtained as

$$\rho_1^{(i)} = \begin{cases} d(\mathbf{a}_i, \mathbf{a}_m), & \text{if } \exists r(\mathbf{a}_i, \mathbf{a}_m) \\ & = \inf\left\{r\left(\mathbf{a}_i, \mathbf{a}_j\right), j \neq i : r\left(\mathbf{a}_i, \mathbf{a}_j\right) > r\left(\mathbf{a}_i, \mathbf{p}\right)\right\}, \\ 0, & \text{otherwise,} \end{cases}$$

$$\rho_2^{(i)} = \begin{cases} d(\mathbf{a}_i, \mathbf{a}_n), & \text{if } \exists r(\mathbf{a}_i, \mathbf{a}_n) \\ & = \sup\left\{r\left(\mathbf{a}_i, \mathbf{a}_j\right), j \neq i : r\left(\mathbf{a}_i, \mathbf{a}_j\right) < r\left(\mathbf{a}_i, \mathbf{p}\right)\right\}, \\ \infty, & \text{otherwise,} \end{cases} \tag{3}$$

where $\inf(S)$ and $\sup(S)$ denote the infimum and supremum of the set S, respectively.

After repeating this procedure for all the anchors, the node is found to be located on the intersection of a set of rings $R(\mathbf{a}_i, \rho_1^{(i)}, \rho_2^{(i)})$, $i = 1, 2, \ldots, N$, of the form (2); finally, the node position is estimated as the centroid of the intersection region. Notice that unlike range-based methods, range-free localization techniques cannot obtain the exact node position $\mathbf{p}$, even in the absence of measurement errors, because they only provide bounds for the location; however, these bounds tend to be tighter as the number of anchors N increases.

With actual measurements, the condition (1) does not hold for every pair of nodes because the radio channel is usually anisotropic, so that not all the rings (2) have a common intersection. The compromise solution in such cases is to assume the UN to be in the region of the plane where most of the rings intersect. This is equivalent to assume that every anchor "votes" for a given ring as a candidate to hold the UN, and the region of the plane that gets the higher number of votes is finally elected. Such voting strategy has the added benefit of providing a good degree of robustness to attacks to the localization process triggered by malicious anchors [19, 20].

On the other hand, the achieved number of votes (i.e., intersecting rings) for the region of the plane finally elected is also an indicator of the "degree of success" of the localization process: a high value for this number (relative to its absolute maximum, i.e., the number of anchors N) implies that RSS measurements are highly correlated to actual distances between nodes, so that the monotonicity constraint (1) is fulfilled in most situations. This fact is illustrated in Figure 1, where we can see examples of two extreme cases: Figure 1(a) represents the distribution of the number of votes when the node to be located receives RSS measurements that are independent of distances, while Figure 1(b) illustrates a situation where RSSs are deterministically related to distances; notice the presence of a sharp peak in this latter case, highlighting the area where the node is located.

The ROCRSSI algorithm, unlike other range-free approaches, does not require any special hardware at the nodes (like directive antennas) and its implementation does not depend on parameters that are somewhat imprecisely defined such as the "communication range," commonly employed by range-free methods based on connectivity.

4. Attack Model

We will assume the existence of an adversary who tries to deceive both the location and neighborhood discovery protocols by forcing a remote compromised node to appear as a neighbor of the local network nodes. To accomplish this, the attacker uses a wormhole link with two endpoints: one in the vicinity of the anchor nodes, and the other within the radio range of the compromised node (see Figure 2); the wormhole local node captures beaconing packets sent from the anchor nodes and tunnels them to the wormhole remote node through a dedicated high-speed link, so that they arrive unmodified at the compromised node. This latter node, then, applies the localization procedure using these packets as if they came directly from the anchors, therefore resulting in a fake position within the deployment area of the local network. As the wormhole nodes act as simple relays and do not manipulate the information contained in the packets, wormhole attacks resist defensive measures solely based on cryptographic protocols.

Once the compromised node is falsely positioned, the network can become vulnerable to different exploits. For instance, the compromised node could inadvertently inject misleading information into the local network or obtain sensitive data from other nodes and flow them through the wormhole link. Another possibility for an adversary comes from the fact that the wormhole local node can be easily masqueraded as an authenticated local node by impersonating the compromised node; in this way, anyone who physically bears the wormhole local node could gain access to restricted areas or secret information [2].

The model of Figure 2, in spite of its simplicity, captures the essential mechanism of a wormhole attack to LD and ND protocols. Ironically, however, most existing wormhole detection schemes cannot cope with this simple attack for several reasons as follows.

(i) The simple scenario of Figure 2 assumes that in a normal situation (no attack), all the active nodes are neighbors; this precludes the use of secure LD or ND techniques solely based on connectivity information or hop counts. Obviously, methods for wormhole detection based on the analysis of "network layer" parameters (routes, traffic, etc.) are also inapplicable.

(ii) The compromised node only communicates with the remote wormhole node, so it cannot get cooperation from "real" neighbors in the localization process or the detection of the attack.

(iii) A wormhole attack is undetectable by "network-based" localization techniques [21]: if the position of the node is obtained from signals received by the anchors, the compromised node will be always located at the position of the wormhole local node. Therefore, the LD procedure should be performed at the unlocalized node, using data it received from the anchors, because the unlocalized node is the only one that can detect inconsistencies caused by a wormhole attack.

On the other hand, the model of Figure 2 is simple enough to allow the application of standard tools of statistical decision theory to the problems of node localization and wormhole detection.

As a wormhole attack challenges higher-level protocols, most effective procedures to detect such attacks are based on looking for inconsistencies in measurements performed at the physical layer level. In the next sections, we develop different detection strategies that analyze the RSS values measured by the nodes interacting in the localization procedure.

5. Wormhole Detection Using RSS: Parametric Approach

Any wormhole detection procedure can be stated as a binary hypothesis testing problem: given a vector of N RSS observations $\mathbf{r} = [r_1, r_2, \ldots, r_N]^T$, we must decide between hypothesis H_0 (no wormhole is present) and H_1 (a wormhole attack is active). However, to formalize the test we need a suitable statistical description of the observations. In the sequel, we will use the standard log-distance path-loss model [22] that links RSS values (in logarithmic scale) to distances as

$$r(\mathbf{x}, \mathbf{y}) = K - 10\alpha \log_{10} d(\mathbf{x}, \mathbf{y}) + e, \tag{4}$$

where $\mathbf{x}$ and $\mathbf{y}$ are the positions of the transmitter and receiver, respectively, K is the mean received power (in dBm) at unit distance, α is the path-loss exponent (which depends on the environment), and e is a zero-mean Gaussian random variable with standard deviation σ (in dB) that takes into account shadowing effects. Therefore, $r(\mathbf{x}, \mathbf{y})$ is also a Gaussian random variable with standard deviation σ and mean $\mu(\mathbf{x}, \mathbf{y})$, with

$$\mu(\mathbf{x}, \mathbf{y}) = K - 10\alpha \log_{10} d(\mathbf{x}, \mathbf{y}). \tag{5}$$

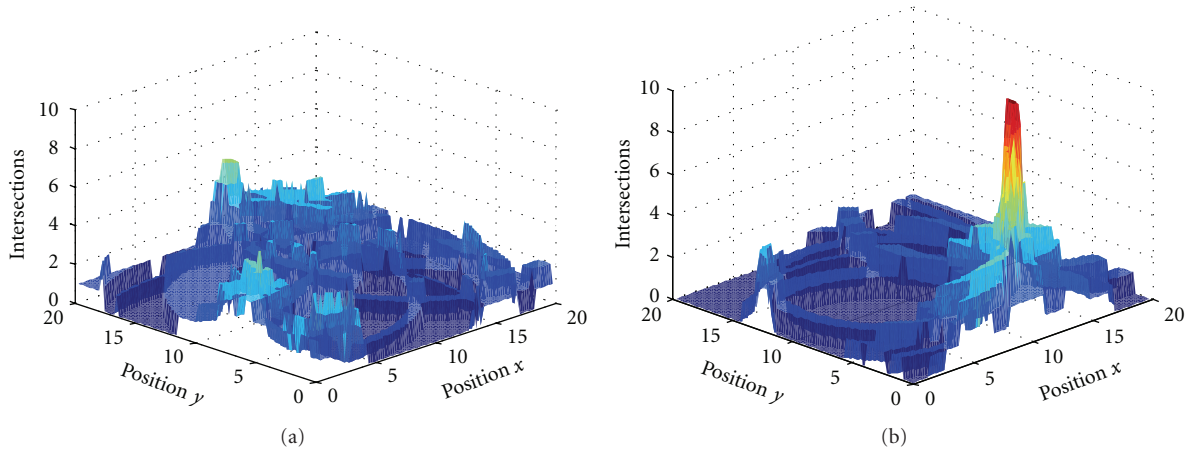


FIGURE 1: Spatial distributions of the number of intersecting rings with $N = 10$ anchors. (a) RSS measurements independent of distances. (b) RSS measurements inversely related to distances.

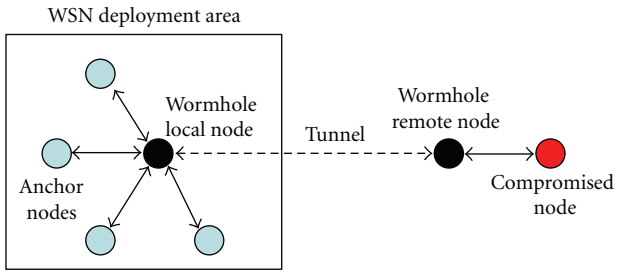


FIGURE 2: Wormhole attack to location and neighbor discovery.

Now, assuming that the observations are independent and identically distributed (IID), the distribution of $\mathbf{r}$ is multivariate normal with mean vector $\boldsymbol{\mu} = [\mu_1, \mu_2, \ldots, \mu_N]^T$ and covariance matrix $\sigma^2\mathbf{I}$, where $\mathbf{I}$ is the identity matrix, so that the joint probability density function (PDF) of the RSS measurements is

$$f(\mathbf{r};\boldsymbol{\mu}) = (2\pi\sigma^2)^{-N/2} \exp\left[-\frac{1}{2\sigma^2}(\mathbf{r}-\boldsymbol{\mu})^T(\mathbf{r}-\boldsymbol{\mu})\right], \quad (6)$$

where the superscript T denotes "transpose." The assumption of IID observations is valid whenever they are associated to transmitters and/or receivers located at different positions and shadow fading is spatially uncorrelated.

According to (5), the only parameter of (6) that depends on the position is $\boldsymbol{\mu}$, so we will formulate the wormhole detection problem as a test of the mean vector of $\mathbf{r}$:

$$\begin{aligned} H_0 &: \boldsymbol{\mu} = \boldsymbol{\mu}_0, \\ H_1 &: \boldsymbol{\mu} \neq \boldsymbol{\mu}_0, \end{aligned} \quad (7)$$

where $\boldsymbol{\mu}_0$ is determined assuming there is no wormhole present.

Now, depending on the origin of the measurements, we can define two different tests. The first one is carried out by the unlocalized node, which performs the localization and wormhole detection processes simultaneously, using RSS values obtained from packets supposedly transmitted by the anchors. The second strategy can be applied after the node is localized and is performed by the anchors, which analyze the RSS measurements obtained from packets supposedly transmitted by the localized node. Both schemes are presented in Sections 5.1 and 5.2, respectively.

5.1. Simultaneous Localization and Wormhole Detection: Likelihood Ratio Test. In this scheme, the anchors broadcast beaconing packets containing their positions, conveniently enciphered and authenticated to prevent other kinds of attacks. These packets are intended to be received by the unlocalized node, which measures their RSS values and then decrypts them to obtain the positions of the anchors. As stated previously, assuming that the statistical model for the RSS observations (6) is valid, then the wormhole detection procedure can be formulated as a hypothesis testing problem of the form (7), where the measurements $\mathbf{r} = [r_1, r_2, \ldots, r_N]^T$ are, in our case, collected by the unlocalized node.

Therefore, if the hypothesis H_0 (no wormhole) is true, then the observations are RSS values of packets transmitted by the anchors at known positions $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N\}$ (see Figure 3(a)), so that we have the null hypothesis

$$H_0 : r_i = r(\mathbf{a}_i, \mathbf{p}), \quad i = 1, 2, \ldots, N \quad (8)$$

and according to (5), the elements of vector $\boldsymbol{\mu}_0$ in (7) are

$$\mu_{0,i} = K - 10\alpha \log_{10} d(\mathbf{a}_i, \mathbf{p}), \quad i = 1, 2, \ldots, N. \quad (9)$$

However, under H_1 (wormhole attack), the packets obtained by the unlocalized node come from the remote wormhole node, as shown in Figure 2; therefore, the RSS values for these packets will be totally unrelated to the anchors positions We will further assume that the remote wormhole node "randomizes" the observations (e.g., by changing its transmitted power) to avoid that they all take the same value and so circumvent a trivial detection; thus, the assumption of IID observations also holds true under H_1.

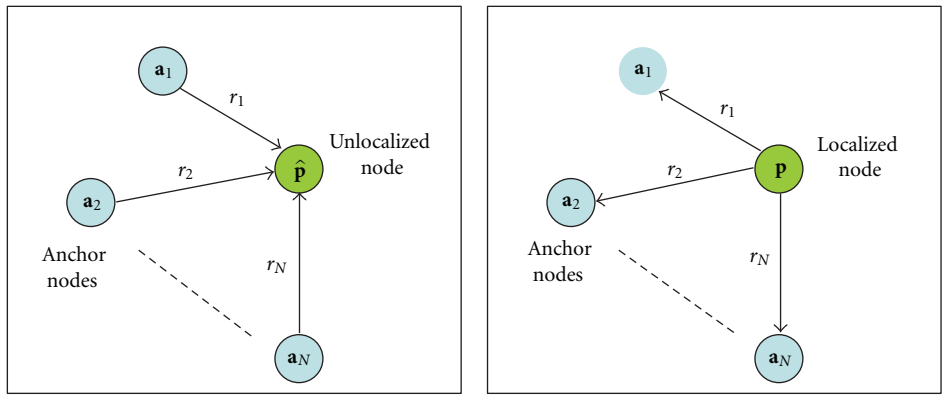


Figure 3: Scenarios for secure neighbor discovery assuming no wormhole is present. (a) Simultaneous localization and wormhole detection. (b) Wormhole detection after localization.

Notice that, as the position of the node $\mathbf{p}$ is unknown, both H_0 and H_1 of (7) are composite hypotheses. Therefore, we can obtain the likelihood ratio test (LRT) [23] as

$$\text{Decide } H_1 \,(\text{wormhole present}) \text{ iff } \Lambda(\mathbf{r}) > \eta, \tag{10}$$

where $\Lambda(\mathbf{r})$ is the likelihood ratio

$$\Lambda(\mathbf{r}) = \frac{\max_{\boldsymbol{\mu}} f(\mathbf{r};\boldsymbol{\mu})}{\max_{\boldsymbol{\mu}_0} f\left(\mathbf{r};\boldsymbol{\mu}_0\right)} \tag{11}$$

and η is a threshold selected so that we have a given probability of false alarm (PFA). Taking into account (6) and (9), we have

$$f\left(\mathbf{r};\boldsymbol{\mu}_0\right) = \left(2\pi\sigma^2\right)^{-N/2} \exp\left[-\frac{1}{2\sigma^2} V(\mathbf{p})\right] \tag{12}$$

with

$$V(\mathbf{p}) = \sum_{i=1}^{N} \left[r_i - K + 10\alpha \log_{10} d(\mathbf{a}_i, \mathbf{p})\right]^2. \tag{13}$$

The numerator of (11) is easily obtained, according to (6), as

$$\max_{\boldsymbol{\mu}} f(\mathbf{r};\boldsymbol{\mu}) = \left(2\pi\sigma^2\right)^{-N/2} \tag{14}$$

while the denominator of (11) is, according to (12),

$$\max_{\boldsymbol{\mu}_0} f\left(\mathbf{r};\boldsymbol{\mu}_0\right) = \left(2\pi\sigma^2\right)^{-N/2} \exp\left[-\frac{1}{2\sigma^2} V(\hat{\mathbf{p}})\right], \tag{15}$$

where $\hat{\mathbf{p}}$ is the maximum likelihood estimate (MLE) of $\mathbf{p}$ under H_0, defined as

$$\hat{\mathbf{p}} = \arg\max_{\mathbf{p}} f\left(\mathbf{r};\boldsymbol{\mu}_0\right). \tag{16}$$

Taking into account the inverse relationship between $f(\mathbf{r};\boldsymbol{\mu}_0)$ and $V(\mathbf{p})$, (16) can be also expressed as

$$\hat{\mathbf{p}} = \arg\min_{\mathbf{p}} V(\mathbf{p}) \tag{17}$$

so that $\hat{\mathbf{p}}$ is obtained as the solution of a nonlinear least square (NLS) problem. Finding the global solution of (17) is, in general, a difficult optimization problem because of the existence of multiple local minima in the objective function. Therefore, it is customary to resort to simpler suboptimal alternatives to the exact MLE that guarantee a single local minimum [24, 25].

Now, taking into account (11), (14), and (15), we can compute the logarithm of the likelihood ratio as

$$\ln \Lambda(\mathbf{r}) = \frac{V(\hat{\mathbf{p}})}{2\sigma^2} \tag{18}$$

so that a test equivalent to (10) is

$$\text{Decide } H_1 \text{ iff } V(\hat{\mathbf{p}}) > \eta', \tag{19}$$

where η' is another suitable threshold, selected so that

$$P\left[V(\hat{\mathbf{p}}) > \eta' \mid H_0\right] = P_{\text{FA}} \tag{20}$$

with P_{FA} the probability of false alarm. The LRT is summarized in Algorithm 1.

We can see from (13) that $V(\hat{\mathbf{p}})$ is the sum of the squared residuals, so it represents a measure of the "quality" of the MLE $\hat{\mathbf{p}}$.

5.2. Wormhole Detection after Localization: Likelihood Ratio Test. Another wormhole detection strategy could be implemented after a given node has completed the localization procedure, and as a result of this, it has obtained a position within the local network deployment area. The idea now is to use the anchor nodes to check the validity of the node location.

To accomplish this, the localized node broadcasts cryptographically secured packets containing its position $\mathbf{p}$ to be verified. These packets are received by the anchors, which use them to obtain RSS measurements and the declared node position. So, in this case, the observations $\mathbf{r} = [r_1, r_2, \ldots, r_N]^T$ are collected by the anchors and under H_0 (no wormhole), correspond to the RSS values of packets

Inputs:
Set of trustworthy anchor positions: $\{\mathbf{a}_i, i = 1, 2, \ldots, N\}$
Set of untrustworthy anchor to node RSSs: $\{r_i = r(\mathbf{a}_i, \mathbf{p}), i = 1, 2, \ldots, N\}$
Parameters of the path-loss model: K and α.
Detection threshold: η'
Steps:
(1) Obtain $\hat{\mathbf{p}}$ as the maximum likelihood estimate (MLE) of the position of the node using (17) and (13).
(2) Compute the test statistic $V(\hat{\mathbf{p}})$ using (13).
(3) **if** $V(\hat{\mathbf{p}}) > \eta'$ then
(4) **set** *wormhole_flag* ←*true*
(5) **else**
(6) **set** *wormhole_flag* ← *false*
(7) **end if**
(8) **return** *wormhole_flag* and estimated position $\hat{\mathbf{p}}$

Algorithm 1: Simultaneous localization and wormhole detection. Parametric approach: likelihood ratio test.

transmitted by the node at position $\mathbf{p}$ and received by the anchors at positions $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N\}$ (see Figure 3(b)). Therefore, we have the null hypothesis

$$H_0 : r_i = r(\mathbf{p}, \mathbf{a}_i), \quad i = 1, 2, \ldots, N, \tag{21}$$

and according to (5) and taking into account that $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$, for all $\mathbf{x}, \mathbf{y}$, the elements of vector $\boldsymbol{\mu}_0$ are also given by (9).

On the other hand, under H_1 (wormhole attack), the packets received by the anchors are transmitted by the local wormhole node, as shown in Figure 2; therefore, the RSS values for these packets will be unrelated to the declared position of the compromised node $\mathbf{p}$.

Therefore, the only difference with the previous case is that now the position of the node $\mathbf{p}$ is known, so H_0 is a simple hypothesis and the likelihood ratio is

$$\Lambda(\mathbf{r}) = \frac{\max_{\boldsymbol{\mu}} f(\mathbf{r}; \boldsymbol{\mu})}{f\left(\mathbf{r}; \boldsymbol{\mu}_0\right)}, \tag{22}$$

where $f(\mathbf{r}; \boldsymbol{\mu})$ and $f(\mathbf{r}; \boldsymbol{\mu}_0)$ are given by (6) and (12), respectively.

Following analogous steps to the previous section, we arrive at a test similar to (19) but using the reported position instead of the MLE (see Algorithm 2):

$$\text{Decide } H_1 \text{ iff } V(\mathbf{p}) > \eta'', \tag{23}$$

where $V(\mathbf{p})$ was defined in (13) and η'' is chosen so that

$$P[V(\mathbf{p}) > \eta'' \mid H_0] = P_{\text{FA}}. \tag{24}$$

Again, the test statistic $V(\mathbf{p})$ is a measure of "goodness of fit" of the declared position to the observations.

6. Wormhole Detection Using RSS: Nonparametric Approach

The detection strategies of Section 5 assume the existence of a well-defined measurement model that describes the statistical relationship between observed RSS values and distances. However, in most instances, such model can only be stated under idealized conditions or is tied to a specific scenario; in this latter case, estimating its parameters often requires a costly calibration phase which must be repeated every time the environmental conditions change.

Therefore, it would be desirable to devise wormhole detection procedures that are "nonparametric" in the sense that unlike the test (7), these strategies do not impose a particular distribution for the observations; thus, such tests will be robust against departures from any predefined model. In particular, we will base our derivations of nonparametric detection schemes on the underlying ideas of the range-free positioning techniques described in Section 3.

As above, depending on the source of the measurements, we will derive a procedure for simultaneous localization and wormhole detection performed by the unlocalized node, using RSS values obtained from packets transmitted by the anchors, and a postlocalization wormhole detection scheme performed by the anchors, employing RSS measurements obtained from packets transmitted by the localized node. Both schemes are presented in Sections 6.1 and 6.2, respectively.

6.1. Simultaneous Localization and Wormhole Detection: DWARFLoc. We can check the presence of a wormhole without assuming any specific model for the observations by exploiting the fact that under no attack, the RSS values collected by the unlocalized node will be related to the distances from the node to the anchors, no matter which is the exact form of this relationship; on the other hand, if a wormhole is present, the RSS values measured by the compromised node are totally unrelated to its actual position.

Thus, under a wormhole attack and assuming that the compromised node uses the ROCRSSI scheme described in Section 3 to localize itself, it is very unlikely for the rings provided by the anchor nodes to share a common intersection, even in the absence of measurement errors; so, if a voting strategy is adopted to estimate the unknown node position, the number of votes received by any region in the plane will be well below the maximum attainable score (see

Inputs:
Set of trustworthy anchor positions: $\{\mathbf{a}_i, i = 1, 2, \ldots, N\}$
Untrustworthy node position: $\mathbf{p}$
Set of untrustworthy node to anchor RSSs: $\{r_i = r(\mathbf{p}, \mathbf{a}_i), i = 1, 2, \ldots, N\}$
Parameters of the path-loss model: K and α
Detection threshold: η''
Steps:
(1) Obtain the anchor to node distances $\{d(\mathbf{a}_i, \mathbf{p}), i = 1, 2, \ldots, N\}$.
(2) Compute the test statistic $V(\mathbf{p})$ using (13).
(3) **if** $V(\mathbf{p}) > \eta''$ then
(4) **set** *wormhole_flag* ← *true*
(5) **else**
(6) **set** *wormhole_flag* ← *false*
(7) **end if**
(8) **return** *wormhole_flag*

Algorithm 2: Detection after localization. Parametric approach: likelihood ratio test.

Figure 1(a)). On the other hand, if no wormhole is present, we should expect that most anchors agree on the existence of a region of the plane that satisfies the set of constraints (2); this region, therefore, will receive a high number of votes (relative to the number of anchors), as Figure 1(b) illustrates. For these reasons, the test statistic proposed for this nonparametric detection strategy is the deviation of the maximum number of votes attained by any region of the plane from the average number of votes.

Therefore, in this scheme the anchor nodes broadcast beaconing packets that contain their positions and the RSSs they measure for packets transmitted by other anchor nodes; such packets should be conveniently enciphered and authenticated. Then, the unlocalized node collects and decrypts the beaconing packets and computes RSS values for them (see Figure 3(a)); these measurements, along with the positions of the anchors and the anchor-to-anchor RSSs, are used to estimate the position of the node, via the ROCRSSI method. The quality of the estimated position is determined by the number of votes it received, and if this number (after mean centering) is above a predefined threshold, the localization process is considered valid; otherwise, an attack is presumed and the unlocated node refrains from joining the network. As usual, the detection threshold is selected to obtain a given PFA. The whole DWARFLoc procedure is described in Algorithm 3.

6.2. Wormhole Detection after Localization: DWARFTest. Once the node is successfully located, we can proceed to verify the validity of the node position $\mathbf{p}$ by reversing the previous roles of the tested node and the anchor nodes (see Figure 3(b)): now the former broadcasts packets containing its estimated location, while the latter receive these transmissions, compute RSS values, and use them to look for possible violations of the monotonicity constraint (1). If the tested node has been compromised by a wormhole attack like that of Figure 2, the source of those packets will be the wormhole local node, whose position is, with a high probability, different from that reported by the compromised node, so that many of the anchor nodes will find that the measured RSSs do not agree with the expected ones. Obviously, beside the anchor nodes, any other node whose position has been previously validated can also participate in this wormhole detection procedure. Notice also that the RSS values collected by the anchors should be transmitted to a central node in order to process them.

As a measure of dissimilarity between distances and RSS measurements, we have used a slight modification of the classical Kendall tau distance [26], which is a metric that counts the number of pairwise disagreements between two lists. In our case, the test statistic counts the number of violations of the monotonicity constraint (1) for every possible pair of node-to-anchor distances and their corresponding measured RSS values as

$$\tau(\mathbf{p}) = \Big|\Big\{(i,j), i<j : \Big(d(\mathbf{p},\mathbf{a}_i) < d\Big(\mathbf{p},\mathbf{a}_j\Big) \wedge r(\mathbf{p},\mathbf{a}_i) < r\Big(\mathbf{p},\mathbf{a}_j\Big)\Big) \vee \Big(d(\mathbf{p},\mathbf{a}_i) > d\Big(\mathbf{p},\mathbf{a}_j\Big) \wedge r(\mathbf{p},\mathbf{a}_i) > r\Big(\mathbf{p},\mathbf{a}_j\Big)\Big)\Big\}\Big|, \tag{25}$$

where $|S|$ denotes the cardinal number of a set S.

As the test statistic $\tau(\mathbf{p})$ is a discrete random variable (it only takes integer values), the decision procedure should include two parameters to exactly obtain a predefined PFA: an integer detection threshold η and a real number γ ($0 \leq \gamma \leq 1$), such that

$$P[\tau(\mathbf{p}) > \eta \mid H_0] + \gamma P[\tau(\mathbf{p}) = \eta \mid H_0] = P_{\mathrm{FA}}, \tag{26}$$

where P_{FA} is the desired probability of false alarm. The steps to implement the DWARFTest procedure are illustrated in Algorithm 4.

7. Simulation Results

We have conducted some simulations to evaluate and compare the performance of the wormhole detection strategies described in Sections 5 and 6. The simulated WSN is composed of a set of anchor nodes whose positions are uniformly distributed in a square room of 20 m × 20 m.

Inputs:
Set of anchor positions: $\{\mathbf{a}_i, i = 1, 2, \ldots, N\}$
Set of untrustworthy anchor to node RSSs: $\{r(\mathbf{a}_i, \mathbf{p}), i = 1, 2, \ldots, N\}$
Set of trustworthy anchor to anchor RSSs: $\{r(\mathbf{a}_i, \mathbf{a}_j), i = 1, 2, \ldots, N; j = 1, 2, \ldots, N; i \neq j\}$
Detection threshold: η
Steps:
(1) Define a grid $\mathbf{G}$ of L points in the plane, covering the WSN deployment region and an array $\mathbf{V}$ of L counters.
(2) **set** $\mathbf{V} \leftarrow \mathbf{0}$
(3) **for** every anchor $\mathbf{a}_i, i = 1, 2, \ldots, N$ **do**
(4) Obtain a ring $R(\mathbf{a}_i, \rho_1^{(i)}, \rho_2^{(i)})$ of the form (2) that should ideally contain the node position, using (3)
(5) **for** every point of the grid $\mathbf{g} \in \mathbf{G}$ **do**
(6) **if** $\mathbf{g} \in R(\mathbf{a}_i, r_1^{(i)}, r_2^{(i)})$ **then**
(7) Increment counter of votes for point $\mathbf{g}$: $\mathbf{V}(\mathbf{g}) \leftarrow \mathbf{V}(\mathbf{g}) + 1$
(8) **end if**
(9) **end for**
(10) **end for**
(11) Obtain the intersection region as the set of grid points with maximum number of "votes":

$$v_M = \max_{\mathbf{g} \in \mathbf{G}} \mathbf{V}(\mathbf{g})$$
$$\mathbf{M} = \{\mathbf{g} \in \mathbf{G} : \mathbf{V}(\mathbf{g}) == v_M\}$$

(12) Estimate the position of the node as the centroid of the intersection area:

$$\hat{\mathbf{p}} = \frac{\mathbf{1}}{|\mathbf{M}|} \sum_{\mathbf{g} \in \mathbf{M}} \mathbf{g}$$

(13) Compute the sample mean of the number of votes:

$$\overline{v} = \frac{1}{L} \sum_{\mathbf{g} \in \mathbf{G}} \mathbf{V}(\mathbf{g})$$

(14) **if** $v_M - \overline{v} \leq \eta$ then
(15) **set** *wormhole_flag* $\leftarrow$ *true*
(16) **else**
(17) **set** *wormhole_flag* $\leftarrow$ *false*
(18) **end if**
(19) **return** *wormhole_flag* and estimated position $\hat{\mathbf{p}}$

Algorithm 3: Simultaneous localization and wormhole detection. Nonparametric approach: DWARFLoc.

Inputs:
Set of trustworthy anchor positions: $\{\mathbf{a}_i, i = 1, 2, \ldots, N\}$
Untrustworthy node position: $\mathbf{p}$
Set of untrustworthy node to anchor RSSs: $\{r(\mathbf{p}, \mathbf{a}_i), i = 1, 2, \ldots, N\}$
Detection threshold and "PFA adjustment" parameter: η, γ
Steps:
(1) Obtain the node to anchor distances $\{d(\mathbf{p}, \mathbf{a}_i), i = 1, 2, \ldots, N\}$.
(2) Compute the test statistic $\tau(\mathbf{p})$, using (25)
(3) **if** $\tau(\mathbf{p}) > \eta$ then
(4) **set** *wormhole_flag* $\leftarrow$ *true*
(5) **else if** $\tau(\mathbf{p}) = \eta$
(6) **set** *wormhole_flag* $\leftarrow$ *true* with probability γ
(7) **else**
(8) **set** *wormhole_flag* $\leftarrow$ *true*
(9) **end if**
(10) **return** *wormhole_flag*

Algorithm 4: Wormhole detection after localization. Nonparametric approach: DWARFTest.

For RSS values, we have assumed the log-distance path-loss model (4) for which we set $\alpha = 3$ as a typical value for indoor environments.

The range-free localization scheme uses a square grid of 20×20 elements, which implies a spatial resolution of 1 m in the proposed scenario. The range-based (parametric) approach uses as an approximation for the MLE the best linear unbiased estimator (BLUE) of the node position, because it is much simpler to implement than the exact MLE and its variance is close to the Cramér-Rao lower bound [25].

A wormhole attack is simulated according to the model of Figure 2. The distance between the wormhole remote node and the compromised node, $d(\mathbf{w}, \mathbf{c})$, is randomly chosen, and both nodes are assumed to be located beyond the radio range of any other WSN node. To avoid a trivial detection, the remote wormhole node performs random changes in its transmitted power, so that the RSS values measured by the compromised node are obtained as

$$r_i^c = K - 10\alpha \log_{10} d(\mathbf{w}, \mathbf{c}) + e + u_i, \quad i = 1, 2, \ldots, N, \tag{27}$$

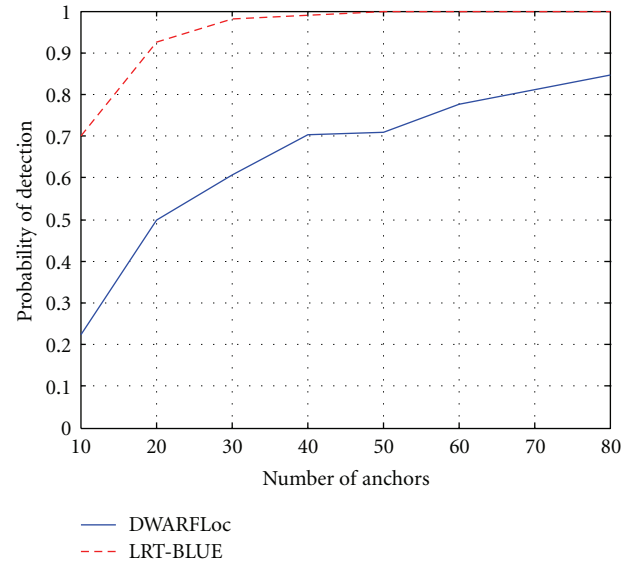
where $d(\mathbf{w}, \mathbf{c})$ is uniformly distributed between 0 and 20 m, e is a zero-mean Gaussian random variable with standard deviation σ, and $\{u_i, i = 1, 2, \ldots, N\}$ are IID random variables with uniform distribution in the interval $(-6, 6)$. These RSSs are first processed by the simultaneous detection and localization schemes of Sections 5.1 and 6.1.

Once the node has been located, the detection procedures of Sections 5.2 and 6.2 are started and the tested node begins to broadcast its estimated position. However, according to Figure 2, if this node has been compromised by a wormhole attack, the RSS values measured by the anchors are related to their distances to the wormhole local node, because this node is acting as a repeater.

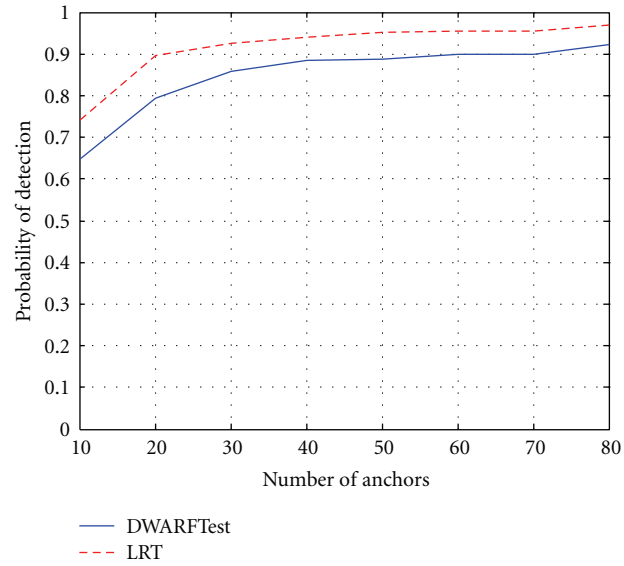
To determine the detection thresholds for the tests, we have also simulated the scenarios of Figure 3, using a reference node whose position is uniformly distributed in the WSN deployment area. Then, for each of the four tests, the empirical cumulative distribution function (CDF) of the test statistic is used to obtain the critical value that ensures a given PFA.

Some results are represented in Figures 4 and 5, where we have plotted the attained probability of detection for the wormhole detection schemes of Sections 5 and 6 under different situations. The PFA is fixed at 0.05 and we conducted 1000 simulation runs in all cases.

By examining Figures 4(a) and 5(a), we can observe that the parametric approach for simultaneous wormhole detection and localization (LRT-BLUE) performs clearly better than the range-free procedure (DWARFLoc); this was expected, because range-free localization methods do not use *a priori* information about any model for the RSS observed values. However, we can see form Figures 4(b) and 5(b) that the range-free version of the scheme for detection after localization (DWARFTest) competes in performance with its parametric counterpart (LRT) and even surpasses it for high values of the path-loss standard deviation; this is attributable to the rapid degradation of the BLUE estimator when the RSS measurements are subject to significant errors.



(a)



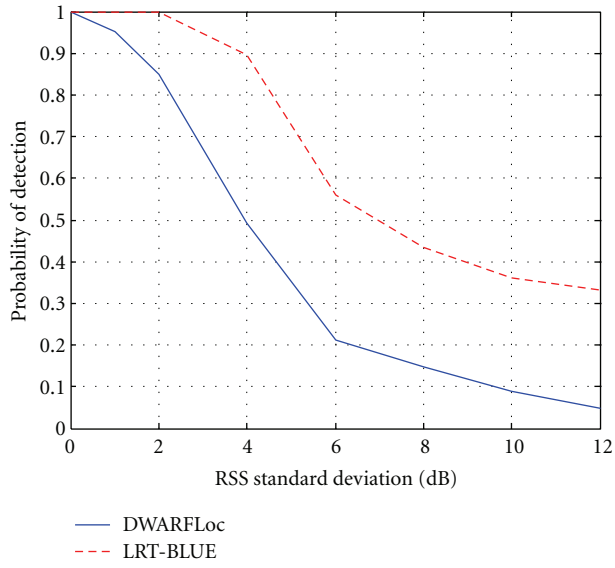
(b)

FIGURE 4: Probability of wormhole detection for the proposed strategies with varying number of anchor nodes ($P_{FA} = 0.05$ and $\sigma = 3$ dB). (a) Simultaneous localization and detection. (b) Detection after localization.

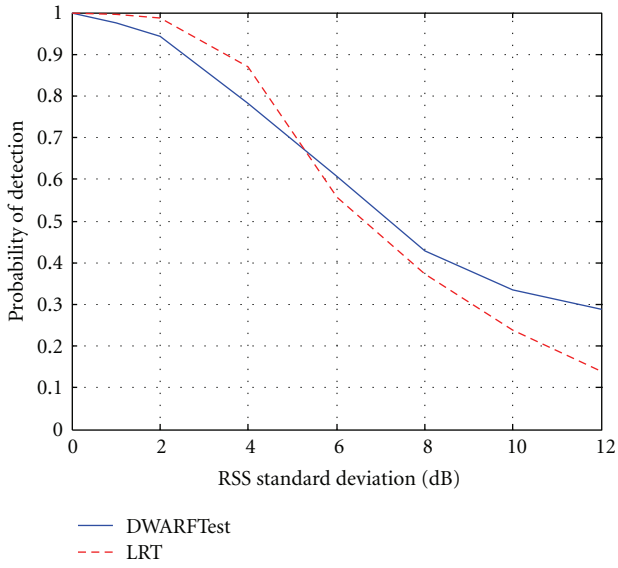
8. Conclusions

In this paper we presented a minimalist model for a wormhole attack to a WSN that can be effectively counteracted by two different detection procedures, based on the underlying ideas of RSS-based range-free localization methods. The first one (DWARFLoc) operates simultaneously with the localization procedure, and the second one (DWARFTest) is a postlocalization detector that tries to validate *a posteriori* the estimated node position. Simulations suggest that DWARFTest has much better detection performance than DWARFLoc but requires more transmissions to be carried out.

Furthermore, assuming that the RSS values follow the standard log-normal path-loss model, we have also derived exact likelihood ratio tests for the detection of a wormhole, which can be used as benchmarks for any other detection scheme.



(a)



(b)

FIGURE 5: Probability of wormhole detection for the proposed strategies with varying path-loss standard deviation ($P_{FA} = 0.05$ and $N = 40$). (a) Simultaneous localization and detection. (b) Detection after localization.

Acknowledgments

This research was partially supported by the Spanish Ministry of Science and Innovation under Grant TEC2009-14219-C03 (AMURA) and the European Commission under Grant FP7-ICT-2009-4-248894 (WHERE2).

References

[1] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60–66, 2008.

[2] P. Papadimitratos, M. Poturalski, P. Schaller et al., "Secure neighborhood discovery: a fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, 2008.

[3] Y. C. Hu and A. Perrig, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–379, 2006.

[4] C. Liu, K. Wu, and T. He, "Sensor localization with ring overlapping based on comparison of received signal strength indicator," in *Proceedings of IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 516–518, October 2004.

[5] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 107–115, May 2007.

[6] T. Giannetsos, T. Dimitriou, and N. R. Prasad, "State of the art on defenses against wormhole attacks in wireless sensor networks," in *Proceedings of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE '09)*, pp. 313–318, May 2009.

[7] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe '04)*, pp. 51–60, October 2004.

[8] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 247–260, 2006.

[9] J. Wu, H. Chen, W. Lou, Z. Wang, and Z. Waang, "Label-based DV-Hop localization againstwormhole attacks in wireless sensor networks," in *Proceedings of the 5th IEEE International Conference on Networking, Architecture and Storage (NAS '10)*, pp. 79–88, July 2010.

[10] L. Lazos, R. Poovendran, and S. Čapkun, "ROPE: Robust position estimation in wireless sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 324–331, April 2005.

[11] S. Čapkun, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[12] L. Lazos and R. Poovendran, "SeRLoc: secure range-independent localization for wireless sensor networks," in *Proceedings of the 2004 ACM Workshop on Wireless Security (WiSe '04)*, pp. 21–30, October 2004.

[13] L. Lazos and R. Poovendran, "HiRLoc: high-resolution robust localization for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233–246, 2006.

[14] Y. Niu, D. Gao, S. Gao, and P. Chen, "A robust localization in wireless sensor networks against wormhole attack," *Journal of Networks*, vol. 7, no. 1, pp. 187–194, 2012.

[15] R. Stoleru, H. Wu, and H. Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1179–1190, 2012.

[16] N. Patwari, A. O. Hero, M. Perkins, N. S. Correal, and R. J. O'Dea, "Relative location estimation in wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 51, no. 8, pp. 2137–2148, 2003.

[17] F. Gustafsson and F. Gunnarsson, "Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 41–53, 2005.

[18] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization and its impact on large scale

sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 4, no. 4, pp. 877–906, 2005.

[19] K. Wu, C. Liu, J. Pan, and D. Huang, "Robust range-free localization in wireless sensor networks," *Mobile Networks and Applications*, vol. 12, no. 5-6, pp. 392–405, 2007.

[20] M. García-Otero, T. Zahariadis, F. Álvarez et al., "Secure geographic routing in ad hoc and wireless sensor networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2010, Article ID 975607, pp. 1–12, 2010.

[21] A. H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: Challenges faced in developing techniques for accurate wireless location information," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 24–40, 2005.

[22] T. S. Rappaport, *Wireless Communications, Principles and Practice*, Prentice Hall, 2nd edition, 2002.

[23] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*, Prentice Hall, 1998.

[24] P. Tarrío, A. M. Bernardos, J. A. Besada, and J. R. Casar, "A new positioning technique for RSS-based localization based on a weighted least squares estimator," in *Proceedings of IEEE International Symposium on Wireless Communication Systems (ISWCS '08)*, pp. 633–637, October 2008.

[25] L. Lin and H. C. So, "Best linear unbiased estimator algorithm for received signal strength based localization," in *Proceedings of the 19th European Signal Processing Conference (EUSIPCO '11)*, pp. 1989–1993, August 2011.

[26] M. Kendall and A. Stuart, *The Advanced Theory of Statistics*, vol. 2, Charles Griffin, 1979.