SeRLoc: Robust Localization for Wireless Sensor Networks

LOUKAS LAZOS and RADHA POOVENDRAN
University of Washington

Many distributed monitoring applications of Wireless Sensor Networks (WSNs) require the location information of a sensor node. In this article, we address the problem of enabling nodes of Wireless Sensor Networks to determine their location in an untrusted environment, known as the *secure localization problem*. We propose a novel range-independent localization algorithm called SeRLoc that is well suited to a resource constrained environment such as a WSN. SeRLoc is a distributed algorithm based on a two-tier network architecture that allows sensors to passively determine their location without interacting with other sensors. We show that SeRLoc is robust against known attacks on a WSNs such as the *wormhole attack*, the *Sybil attack*, and *compromise of network entities* and analytically compute the probability of success for each attack. We also compare the performance of SeRLoc with state-of-the-art range-independent localization schemes and show that SeRLoc has better performance.

Categories and Subject Descriptors: C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Distributed networks, Network topology*

General Terms: Algorithm, Design, Performance, Security

Additional Key Words and Phrases: Range-independent, secure localization, sensor networks

1. INTRODUCTION

Wireless ad hoc sensor networks (WSNs) are expected to be low-cost, self-configurable with no predeployed infrastructure, and easy to deploy. Hence, such networks provide a variety of consumer applications such as emergency rescue, disaster relief, smart homes, and patient monitoring, as well as industrial applications such as distributed structural health monitoring and environmental control, and military applications such as target identification and tracking.

Many of the applications proposed for WSNs require knowledge of the origin of the sensed information. For example, in a disaster relief operation using

This work was supported in part by the following grants: NSF Grant ANI-0093187; ARO Grant DAAD 19-02-1-0242; and ARL CTA Grant DAAD 19-01-2-0011.
Authors' address: L. Lazos, R. Poovendran, Electrical Engineering Department, University of Washington, 434 EE/CSE Bldg., Box 352500, Seattle, WA 98195-2500; email: radha@ee.washington.edu.

a WSN to locate survivors in a collapsed building, it is critical that sensors report monitoring information along with their location. Furthermore, location is assumed to be known in many ad hoc network operations such as routing protocols where a family of geographically-aided algorithms have been proposed [Basagni et al. 1998], or security protocols where location information is used to prevent threats against network services [Hu et al. 2003; Lazos and Poovendran 2003].

Since WSNs may be deployed in hostile environments and operate unsupervised, they are vulnerable to conventional and novel attacks [Hu et al. 2003; Karlof and Wagner 2003] aimed at interrupting the functionality of location-aware applications by exploiting the vulnerabilities of the localization scheme. Though many localization techniques have been proposed for wireless sensor networks, [Bulusu et al. 2000; Nagpal et al. 2003; Niculescu and Nath 2001; He et al. 2003; Savvides et al. 2001; Priyantha et al. 2003; Čapkun et al. 2001], research in secure location estimation is in its infancy.

Since sensors are hardware and power limited, we propose a two-tier network architecture for secure location computation. Our network is comprised of a small number of nodes equipped with special hardware we call *locators* and a large number of resource constrained sensor devices. However, we preserve the characteristics of ad hoc networks by randomly deploying both the sensors and the locators and by allowing them to communicate in an ad hoc mode. Moreover, since distance measurements are susceptible to distance enlargement/reduction, we do not use any such measurements to infer the sensor location. We refer to methods that are not using distance measurements as range-independent localization schemes [He et al. 2003; Nagpal et al. 2003; Niculescu and Nath 2001; Bulusu et al. 2000].

In this article we make the following contributions.

—We introduce the problem of *secure localization* in wireless sensor networks and propose *SeRLoc*, a novel range-independent localization scheme for WSNs based on a two-tier network architecture that achieves decentralized, resource-efficient sensor localization and can accommodate limited sensor mobility.

—We describe well known security threats against WSNs such as the wormhole attack [Hu et al. 2003; Papadimitratos and Haas 2002], the Sybil attack [Douceur 2002; Newsome et al. 2004], and compromise of network entities and provide mechanisms that allow each sensor to determine its location *even* in the presence of these threats. Furthermore, we analytically evaluate the probability of success for each type of attack using *spatial statistics* theory [Cressie 1993].

—Based on our performance evaluation, we show that SeRLoc localizes sensors with higher accuracy than state-of-the-art decentralized range-independent localization schemes [He et al. 2003; Nagpal et al. 2003; Bulusu et al. 2000; Niculescu and Nath 2001] and is robust against varying sources of error.

The remainder of the article is organized as follows. In Section 2, we present related work. In Section 3, we introduce the secure localization problem and

state our network model. Section 4 describes SeRLoc, and Section 5 presents a threat analysis. In Section 6, we evaluate and compare the performance of SeRLoc with other range-independent localization schemes. Section 7 presents our conclusions and future directions.

2. RELATED WORK

While an extensive literature exists on the problem of localization in a trusted environment, secure localization in wireless sensor networks is a fairly unexplored area of research. In fact, to the best of our knowledge ours is the first work to address the problem of estimating the position of the sensors in a hostile environment using range-independent methods. The only other peer reviewed work that addresses the problem of secure position estimation in WSNs is a secure scheme for range-dependent localization [Čapkun and Hubaux 2005] and a preliminary version of our work [Lazos and Poovendran 2004].

Localization schemes can be classified into range-dependent and range-independent-based schemes. In range-dependent schemes, nodes determine their location based on distance or angle estimates to some reference points with known coordinates. Such estimates may be acquired through different methods such as time of arrival (TOA) [Čapkun et al. 2001; Hofmann-Wellenhof et al. 1997], time difference of arrival (TDOA) [Savvides et al. 2001; Priyantha et al. 2003], or angle of arrival (AOA) [Niculescu and Nath 2003].

In the range-independent localization schemes, nodes determine their location without any time, angle, or power measurements. Bulusu et al. [2000] proposed an outdoor localization scheme called *Centroid* where nodes estimate their position as the centroid of the locations of all the beacons transmitted from reference points. The Centroid method is easy to implement and incurs low communication cost. However, it results in a crude approximation of node location. A variant of Centroid using multiple power levels provides much better localization accuracy than Centroid at the expense of increased communication cost [Bulusu 2002].

Niculescu and Nath [2001] proposed *DV-hop* where each node determines the number of hops to nodes with known locations called landmarks, using a distance vector-like method. Once the number of hops to at least three landmarks is known, nodes use an average hop size estimate to determine their distance to the landmarks and apply multilateration to determine their absolute location. Nagpal et al. [2003] followed a similar approach to DV-hop except that they compute the average hop size offline using an approximate formula [Kleinrock and Slivester 1978] with the assumption that every network node has at least a neighborhood of 15 nodes.

He et al. [2003] proposed *APIT*, a range-independent localization scheme that localizes nodes based on beacons transmitted from reference points called anchors and neighbor node information. In APIT, a node s performs a test to determine whether it is inside the triangle defined by a 3-tuple of anchors heard by the node. The test is repeated for all 3-tuples of anchors heard by s, and the location is computed as the center of gravity of the triangles' overlapping region.

Two methods have been proposed that utilize connectivity information to determine the node location. Doherty et al. [2001] formulated a semidefinite program based on the connectivity-induced and angular constraints in order to obtain the optimal position estimates. Shang et al. [2003] used multidimensional scaling to acquire an arbitrary rotation of the network topology. Furthermore, if any three nodes know their location, the network topology can be mapped to the absolute node location. Since both schemes in Doherty et al. [2001] and Shang et al. [2003] are range-based localization techniques, they are not used for comparison in the performance evaluation.

3. PROBLEM STATEMENT AND NETWORK MODEL

3.1 Problem Statement

We study the problem of *enabling nodes of a WSN to determine their location even in the presence of malicious adversaries.* This problem will be referred to as *Secure Localization*. Apart from the secure localization problem, location verification [Sastry et al. 2002], location privacy [Gruteser et al. 2003], and secure location reporting are essential components of any secure location service. Enabling a sensor to securely compute its location is a different problem from securely reporting the location of a sensor, guaranteeing its privacy, or verifying its location claim. Secure location reporting, privacy, and verification, while important areas in their own right, are not addressed in this article. We consider secure localization in the context of the following design goals: (a) decentralized implementation, (b) resource efficiency, (c) range-independence, and (d) robustness against security threats.

3.2 Network Model

Network Setup. We assume a two-tier network architecture with a set of sensors S of unknown location randomly deployed with a density ρ_s within an area $\mathcal{A}$, and a set of specially equipped nodes L we call *locators*, with known location[1] and orientation, also randomly deployed with a density ρ_L.

Antenna Model. We assume that sensors are equipped with omnidirectional antennas and transmit with a power P_s, while locators are equipped with M directional antennas with a directivity gain $G > 1$, and can transmit with a power $P_L > P_s$. Let the signal attenuation over space be proportional to some exponent γ of the distance d between two nodes, times the antenna directivity gain G, ($G = 1$ for omnidirectional antennas), that is, $\frac{P_r}{P_s} = cG^2d^{-\gamma}$, with $2 \leq \gamma \leq 5$, where c denotes a proportionality constant, and P_r denotes the minimum required receive power for communication. If r_{ss} denotes the sensor-to-sensor communication range, and r_{sL} denotes the sensor-to-locator

[1]We presume that the locators acquire their position either through manual insertion or through GPS receivers [Hofmann-Wellenhof et al. 1997]. Though GPS signals can be spoofed, knowledge of the coordinates of several nodes is essential to achieve any kind of node localization for any localization scheme.

Table I.

	Receiver	
Sender	Sensor	Locator
Sensor	r	$rG^{\frac{1}{\gamma}}$
Locator	R	$RG^{\frac{2}{\gamma}}$

(The four communication modes between sensors and locators with each entry indicating the communication range for that mode. The γ denotes the pathloss parameter and G denotes the antenna directivity gain.)

communication range then,

$$\frac{P_r}{P_s} = c(r_{ss})^{-\gamma}, \qquad \frac{P_r}{P_s} = cG(r_{sL})^{-\gamma}. \tag{1}$$

From (1), it follows that $r_{sL} = r_{ss}G^{\frac{1}{\gamma}}$. Similarly, if r_{Ls} denotes the locator-to-sensor communication range, the locator-to-locator communication range r_{LL} is equal to $r_{LL} = r_{Ls}G^{\frac{2}{\gamma}}$. For notational simplicity we will refer to r_{ss} as r, and to r_{Ls} as R. Table I summarizes the four possible communication modes with the appropriate ranges indicated.

To achieve a communication range ratio $\frac{R}{r}$, locators need to transmit with power $P_L = (\frac{R}{r})^{\gamma}(P_s/G)$. Given that sensors are low power devices, locators with higher transmitting power capabilities is a reasonable assumption. A typical sensor has a communication range of $3 \sim 30m$, with a maximum transmission power of $P_s = 0.75mW$ [MICA]. Hence, locators need to transmit with a power $P_g = 75mW$ to achieve a communication range ratio $\frac{R}{r} = 10$ when $\gamma = 2$, even without the use of directional antennas.

Also note that, though the size of directional antennas is a concern for the present operational frequency of sensors, the foreseeable increase in operating frequency will facilitate the use of directional antennas at the locators. At 2.4GHz and a half-wavelength element spacing, the size of an 8-element cylindrical array would be of radius 8cm. At the 5GHz band, the size of an 8-element antenna would have a radius of 3.3cm [Ramanathan 2001]. Since the locators are assumed to be of bigger size than the sensors, equipping locators with directional antennas is a feasible solution.

System Parameters. Since both locators and sensors are randomly and independently deployed, it is essential to select the system parameters so that locators can communicate with sensors. The random deployment of the locators with a density $\rho_L = \frac{|L|}{\mathcal{A}}$ ($|\cdot|$ denotes the cardinality of a set) is equivalent to a sequence of events following a *homogeneous Poisson point process* of rate ρ_L [Cressie 1993]. The random deployment of sensors with a density $\rho_s = \frac{|S|}{\mathcal{A}}$, is equivalent to a random sampling of the area $\mathcal{A}$ with rate ρ_s [Cressie 1993]. Making use of *Spatial Statistics* theory [Cressie 1993], if LH_s denotes the set of locators heard by a sensor s, that is, within range R from s, the probability that s hears exactly k locators, given that the locators are randomly and independently deployed, is given by the Poisson distribution:

$$P(|LH_s| = k) = \frac{(\rho_L \pi R^2)^k}{k!} e^{-\rho_L \pi R^2}. \tag{2}$$

Based on (2), we compute the probability for *every* sensor to hear at least k locators $P(|LH_s| > k)$:

$$P(|LH_s| \geq k, \forall s \in S) = \left(1 - \sum_{i=0}^{k-1} \frac{(\rho_L \pi R^2)^i}{i!} e^{-\rho_L \pi R^2}\right)^{|S|}. \quad (3)$$

Equation (3) allows the choice of ρ_L, R so that a sensor hears at least k locators with any desired probability. The expected number of locators heard by each node, $E(|LH_s|) = \rho_L \pi R^2$, is significantly higher than k. For example, for $R = 20m$, to allow every sensor to hear at least 4 locators with probability $P(|LH_s| \geq 4, \forall s \in S) = 0.99$, we need a $\rho_L = 0.02$ locators/m^2. For $\rho_L = 0.02$ locators/m^2, $E(|LH_s|) = 25.13$. Hence, $P(|LH_s| \geq k, \forall s \in S)$ is a more strict requirement than $E(|LH_s|) = k$. Derivations of (2) and (3) are presented in Appendix 1.

Attacks Not Addressed. In this article, we do not consider attacks against the physical layer such as frequency jamming. Spread spectrum [Pickholtz et al. 1982] and coding [Wicker and Bartz 1994] are known to be efficient mechanisms to shield the physical layer against jamming attacks. Also, we do not consider any attack against the Medium Access Control (MAC) protocol that may lead to a denial-of-service (DoS). In fact, we assume that an adversary will attempt to displace the sensors without being detected and hence, do not examine DoS attacks.

4. SERLOC: SECURE RANGE-INDEPENDENT LOCALIZATION SCHEME

In this section, we present the SEcure Range-independent LOCalization scheme (*SeRLoc*) that enables sensors to determine their location based on beacon information transmitted by the locators even in the presence of security threats.

4.1 Location Determination

In SeRLoc, sensors determine their location based on the beacon information transmitted by the locators. Figure 1(a) illustrates the idea behind the scheme. Each locator transmits different beacons at each antenna sector with each beacon containing (a) the locator's coordinates, and (b) the angles of the antenna boundary lines with respect to a common global axis.

If a sensor receives a beacon transmitted at a specific antenna sector of a locator L_i, it has to be included within that sector. Given the locator-to-sensor communication range R, the coordinates of the transmitting locators, and the sector boundary lines provided by the beacons, each sensor determines its location as the center of gravity (CoG) of the overlapping region of the different sectors. The CoG is the least square error solution given that a sensor can lie with equal probability at any point in the overlapping region. In Figure 1(a), the sensor hears beacons from locators $L_1 \sim L_4$ and determines its position as the CoG of the overlapping region between the four antenna sectors. We now present the algorithmic details of SeRLoc.

Step 1: *Collection of localization information.* In Step 1, the sensor collects information from all the locators that it can hear. A sensor s can hear all locators

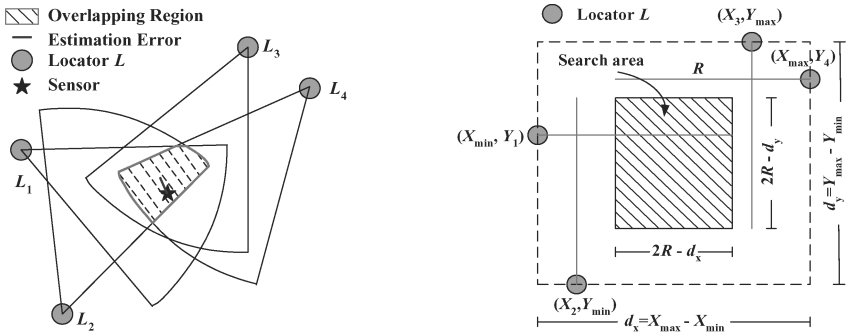

Fig. 1. (a) The sensor hears locators $L_1 \sim L_4$ and estimates its location as the Center of Gravity (CoG) of the overlapping region of the sectors that include it. (b) Determination of the search area.

$L_i \in L$ that lie within a circle of radius R, centered at s.

$$LH_s = \{L_i : \|s - L_i\| \leq R, \quad L_i \in L\}. \tag{4}$$

Step 2: *Search area.* In Step 2, the sensor computes a search area for its location. Let $X_{\min}, Y_{\min}, X_{\max}, Y_{\max}$ denote the minimum and the maximum locator coordinates form the set LH_s.

$$X_{\min} = \min_{L_i \in LH_s} X_i,\ X_{\max} = \max_{L_i \in LH_s} X_i,\ Y_{\min} = \min_{L_i \in LH_s} Y_i,\ Y_{\max} = \max_{L_i \in LH_s} Y_i. \tag{5}$$

Since every locator of set LH_s needs to be within a range R from sensor s, if s can hear locator L_i with coordinates $(X_{\min}, Y_i)$, it has to be located *left* of the vertical boundary of $(X_{\min} + R)$. Similarly, s has to be located *right* of the vertical boundary of $(X_{\max} - R)$, *below* the horizontal boundary of $(Y_{\min} + R)$, and *above* the horizontal boundary of $(Y_{\max} - R)$. The dimensions of the rectangular search area are $(2R - d_x) \times (2R - d_y)$, where d_x, d_y are the horizontal distance $d_x = X_{\max} - X_{\min} \leq 2R$, and the vertical distance $d_y = Y_{\max} - Y_{\min} \leq 2R$, respectively. In Figure 1(b), we show the search area for the network setup in Figure 1(a).

Step 3: *Overlapping region-Majority vote*. In Step 3, sensors determine the overlapping region of all sectors they hear. Since it would be computationally expensive for each sensor to analytically determine the overlapping region based on the line intersections, we employ a grid scoring system that defines the overlapping region based on majority vote.

Grid score table. The sensor places a grid of equally spaced points within the rectangular search area as shown in Figure 2(a). For each grid point, the sensor holds a score in a grid score table with initial values equal to zero. For each grid point, the sensor executes the *grid-sector test* detailed in the following to decide if the grid point is included in a sector heard by a locator of set LH_s. If the grid score test is positive, the sensor increments the corresponding grid score table value by one, otherwise the value remains unchanged. This process is repeated for all locators heard LH_s and all the grid points. The overlapping region is defined by the grid points that have the highest score in the grid score table.

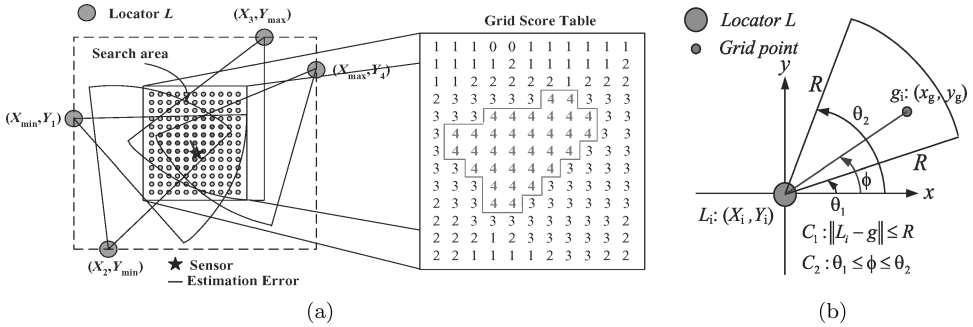

Fig. 2. (a) Steps 3,4: Placement of a grid of equally-spaced points in the search area and the corresponding grid score table. The sensor estimates its position as the centroid of all grid points with the highest score. (b) Step 3: Grid-sector test for a point g of the search area.

In Figure 2(a), we show the grid score table and the corresponding overlapping region.

Note that due to the finite grid resolution, the use of grid points for the definition of the overlapping region induces error in the calculation. The resolution of the grid can be increased to reduce the error at the expense of energy consumption due to the increased processing time.

Grid-sector test. A point $g : (x_g, y_g)$ is included in a sector of angles $[\theta_1, \theta_2]$ originating from locator L_i if it satisfies two conditions:

$$C_1 : \|g - L_i\| \le R, \qquad C_2 : \theta_1 \le \phi \le \theta_2, \tag{6}$$

where ϕ is the slope of the line connecting g with L_i. Note that the sensor *does not have to* perform any angle-of-arrival (AOA) measurements. Both the coordinates of the locators and the grid points are known, and hence the sensor can analytically calculate ϕ. In Figure 2(b), we illustrate the grid-sector test with all angles measured with reference to the x axis.

Step 4: *Location estimation*. The sensor determines its location as the centroid of all the grid points that define the overlapping region:

$$\tilde{s} : (x_{est}, y_{est}) = \left(\frac{1}{n} \sum_{i=1}^{n} x_{g_i}, \frac{1}{n} \sum_{i=1}^{n} y_{g_i} \right), \tag{7}$$

where n is the number of grid points of the overlapping region, and (x_{g_i}, y_{g_i}) are the coordinates of the grid points.

4.2 Accommodating Node Mobility

In the case of a mobile WSN, both the locators and the sensors need to update their current location estimation. While locators can acquire their position using external means (either via satellites, or GPS-enabled fly-over nodes), sensors still rely on locators to update their position. To allow sensors to reestimate their location, locators need to periodically broadcast new beacons with their coordinates and sector information.

4.2.1 *Update Frequency of the Localization Information.* Though sensors passively determine their location via the broadcasted beacons (no information exchange between sensors occurs), we want to broadcast beacons as infrequently as possible in order to minimize the communication overhead at the locators and the computational overhead at the sensors. On the other hand, the updates need to be frequent enough to ensure a localization error within the desired bound. The update frequency of the localization information is determined by the mobility model adopted and the sensor hardware capabilities.

The mobility model indicates how frequently sensors move from one location to the other and need to recompute their location. Though several mobility models can characterize node movement in wireless ad hoc networks [Camp et al. 2002], the mobility of energy-constrained sensors is expected to be rather limited. Hence, it is reasonable to assume a limited mobility model such as the *random waypoint mobility model* [Camp et al. 2002], according to which sensors pause at one location for a specific time interval before moving towards a random direction with a randomly chosen speed between $[v_{\min}, v_{\max}]$. If T_{ps} denotes the pausing interval of a sensor, the minimum rate at which the locators need to broadcast beacons is $f_u \geq \frac{1}{T_{ps}}$, assuming that the pausing interval T_{ps} is much longer than the time interval in which a sensor moves.

Furthermore, mobile sensors may be equipped with hardware capable of providing relative positioning known as dead reckoning. Mobile units can determine their relative position using accelerometers to measure the distance traveled and gyroscopes to measure the change in direction [Yazdi et al. 1998]. A mobile sensor can utilize its last absolute position estimate computed via the beacon information and the relative position measurements to dynamically update its location without new beacons being transmitted. Such relative location estimates are affected by both *systematic* and *nonsystematic* error.

Unlike nonsystematic error that is introduced by random sources, we can compensate for the systematic error by calibrating the system. The calibration can be achieved by comparing the position estimated via dead reckoning with the one estimated via the beacon broadcasting. If the relative positioning system requires calibration every m moves of the mobile sensor, the locators need to broadcast beacons with a frequency not lower than $f_u \geq \frac{1}{mT_{ps}}$.

4.3 Security Mechanisms of SeRLoc

We now describe the security mechanisms of SeRLoc that facilitate sensor localization in the presence of security threats.

Encryption. All beacons transmitted from locators are encrypted with a globally shared symmetric key K_0. In addition, every sensor s shares a symmetric pairwise key $K_s^{L_i}$ with every locator L_i, also preloaded. Since the number of locators deployed is relatively small, the storage requirement at the sensor side is within the storage constraints (a total of $|L|$ keys). For example, mica motes [MICA] have 128Kbytes of programmable flash memory. Using 64-bit RC5 [Rivest 1995] symmetric keys and for a network with 400 locators, a total of 3.2Kbytes of memory is required to store all the keys of the sensor with every locator. In order to save storage space at the locator (locators would have to store

$|S|$ keys), pairwise keys $K_s^{L_i}$ are derived by a master key K_{L_i}, using a pseudo-random function h [Stinson 2002], and the unique sensor ID_s: $K_s^{L_i} = h_{K_{L_i}}(ID_s)$. In Karlof et al. [2004], it was reported that a software implementation of RC5 requires 0.26ms execution time and an increase in energy consumption of 1%–4%. It was also noted that a hardware implementation of RC5 can reduce both the execution time and energy consumption for performing encryption/decryption.

Based on the size of the network deployment region, one can compute the number of locators required for sufficient network coverage. However, the deployment of additional locators may by required in order to improve the localization accuracy at some parts of the network, expand it, or replace locators that have failed. From the security point of view, the problem of adding new locators to the system reduces to the problem of establishing pairwise keys between the new locators and each of the sensors that are already deployed.

Since sensors are hardware and energy limited devices, solutions based on public key cryptography or symmetric key requiring exponentiation [Stinson 2002] cannot be employed. Instead, we can achieve pairwise key establishment between each sensor and the new locators by preloading the sensors with more keys than the number of locators initially deployed. The redundant keys can be later used as pairwise keys between sensors and the new locators. Another approach is to load sensors with some secret quantity only known to each sensor and the authority that deploys the network. The deployment authority can then load the new locator-sensor pairwise keys individually to each sensor, using the secret quantity.

In the case where the network grows large enough so that the pairwise keys of all locators cannot be stored at the sensor's memory, the network can be partitioned into clusters where sensors are loaded only with the pairwise keys shared with the locators within each cluster. Adopting the clustered approach ensures scalability for very large networks. To give a sense of scale, a sensor needs a total of 3.2Kbytes of memory to store 400 64-bit RC5 keys, sufficient for secure communication with 400 locators. If the locator-to-sensor communication range is $R = 100m$ and the 400 locators are randomly dispersed within an area of $4km^2$ ($\rho_L = 10^{-4}$ locators/m^2), each sensor is able to hear $\rho_L \pi R^2 \simeq 3.141$ locators on average. For a network deployed with a sensor density $\rho_s = 0.01$ sensors/m^2 which corresponds to each sensor being able to communicate on average with $\rho_s \pi r^2 \simeq 3.141$ sensors for $r = 10m$, we can accommodate a network of 40,000 sensors. For larger sensor density usually required to guarantee network connectivity and other network properties/functions, the supported sensor network size can be even bigger.

Locator ID Authentication. The use of a globally shared key for the beacon encryption allows a malicious sensor to inject bogus beacons into the network, in the absence of additional security mechanisms. To prevent sensors from broadcasting bogus beacons, we require sensors to authenticate the source of the beacons using *collision-resistant hash functions* [Stinson 2002].

We use the following scheme based on *efficient one-way hash chains* [Lamport 1981], to provide locator ID authentication. Each locator L_i has a unique password PW_i, blinded with the use of a collision-resistant hash function such as SHA1 [Stinson 2002]. Due to the collision resistance property,

it is computationally infeasible for an attacker to find a PW_j, such that $H(PW_i) = H(PW_j),\ PW_i \neq PW_j$. The hash sequence is generated using the following equation:

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

with n being a large number and H^0 never revealed to any sensor. Each sensor is preloaded with a table containing the ID of each locator and the corresponding hash value $H^n(PW_i)$. For a network with 400 locators, we need 9 bits to represent locator IDs. In addition, collision-resistant hash functions such as SHA1 [Stinson 2002] have a 160-bit output. Hence, the storage requirement of the hash table at any sensor is 8.45Kbytes.[2] To reduce the storage needed at the locators, we employ an efficient storage/computation method for hash chains of time/storage complexity $\mathcal{O}(\log^2(n))$ [Coppersmith and Jakobsson 2002].

The jth broadcasted beacon from locator L_i includes the hash value $H^{n-j}(PW_i)$, along with the index j. Every sensor that hears the beacon accepts the message only if $H(H^{n-j+1}(PW_i)) = H^{n-j}(PW_i)$. After verification, the sensor replaces $H^{n-j+1}(PW_i)$ with $H^{n-j}(PW_i)$ in its memory and increases the hash counter by one so as to perform only one hash operation in the reception of the next beacon from the same locator L_i. The index j is included in the beacons so that sensors can resynchronize with the current published hash value in case of loss of some intermediate hash values. The beacon of locator L_i has the following format:

$$L_i :\ \{(X_i, Y_i)\ ||\ (\theta_1, \theta_2)\ ||\ (H^{n-j}(PW_i))\ \|\ j\ \|\ ID_{L_i}\}_{K_0},$$

where $||$ denotes the concatenation operation and $\{m\}_K$ denotes the encryption of message m with key K. Note that our method does not provide end-to-end locator authentication, but only guarantees authenticity for the messages received from locators directly heard to a sensor. This condition is sufficient to secure our localization scheme against possible attacks. The pseudocode for SeRLoc is presented in Figure 3.

5. THREAT ANALYSIS

In this Section, we describe possible security threats against SeRLoc and show that SeRLoc is resilient against these threats. Note that our goal is not to prevent the attacks that may be harmful in many network protocols, but to allow sensors to determine their location, even in the presence of such attacks.

5.1 The Wormhole Attack

5.1.1 *Threat Model.* To mount a wormhole attack, an attacker initially establishes a direct link referred to as a *wormhole link* between two points in the network. Once the wormhole link is established, the attacker eavesdrops messages at one end of the link, referred to as the *origin point*, tunnels them

[2]The required storage at each sensor in order to store 400 64-bit RC5 keys, 400 160-bit SHA1 hash values for secure communication with 400 locators is now 11.65 Kbytes.

SeRLoc: Secure Range-Independent Localization Scheme

L : **broadcast** L_i : $\{ (X_i, Y_i) \,||\, (\theta_1, \theta_2) \,||\, (H^{n-j}(PW_i)) \parallel j \parallel ID_{L_i} \}_{K_0}$

$LH_s = \{L_i : \|s - L_i\| \leq R\} \bigcap \{H(H^{n-j}(PW_i)) = H^{n-j+1}(PW_i)\}$

s : **define** $A_s = [X_{\max} - R,\ X_{\min} + R,\ Y_{\max} - R,\ Y_{\min} + R]$

for k=1:res

  for w=1:res

    $g(k,w) = (x_{g_i}, y_{g_i}) = \left(X_{\max} - R + k\frac{X_{\max} - X_{\min}}{res},\ Y_{\max} - R + w\frac{Y_{\max} - Y_{\min}}{res}\right)$

    for $z = 1 : |LH_s|$

      if $\{\|g(k,w) - L_z\| \leq R\} \bigcap \{\theta_1 \leq \angle g(k,w) \leq \theta_2\}$

        $GST(k,w) = GST(k,w) + 1$

$MG_s = \{g(k,w) : \{k,w\} = \arg\max GST\}$

$$\tilde{s} : (x_{est}, y_{est}) = \left(\frac{1}{|MG_s|}\sum_{i=1}^{|MG_s|} x_{g_i}, \frac{1}{|MG_s|}\sum_{i=1}^{|MG_s|} y_{g_i}\right)$$

Fig. 3. The pseudocode of SeRLoc.

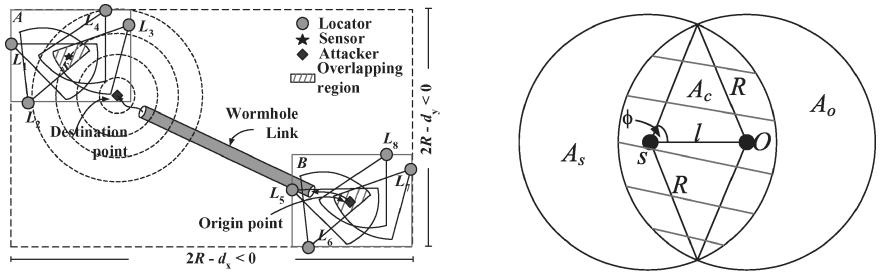

Fig. 4. (a) Wormhole attack: an attacker records beacons in area B, tunnels them via the wormhole link in area A, and rebroadcasts them. (b) Computation of the common area A_c, where locators are heard to both s, O.

through the wormhole link and replays them at the other end, referred to as the *destination point*. The wormhole attack is very difficult to detect since it is launched without compromising any host or the integrity and authenticity of the communication [Hu et al. 2003; Papadimitratos and Haas 2002].

In the case of SeRLoc, an attacker records the beacons transmitted from locators at the origin point and replays them at the destination point, thus providing false localization information to the sensors attacked. In Figure 4(a), the attacker records beacons at region B, tunnels them via the wormhole link in region A, and replays them, thus leading sensor s to believe that it can hear locators $\{L_1 \sim L_8\}$.

5.1.2 *Detecting Wormholes in SeRLoc.* We now show how a sensor can detect a wormhole attack using two properties: the *single message/sector per locator* property and the *communication range constraint* property.

Single Message/Sector per Locator Property. The origin point O of the wormhole attack defines the set of locators LH_s^r replayed to the sensor s under attack.

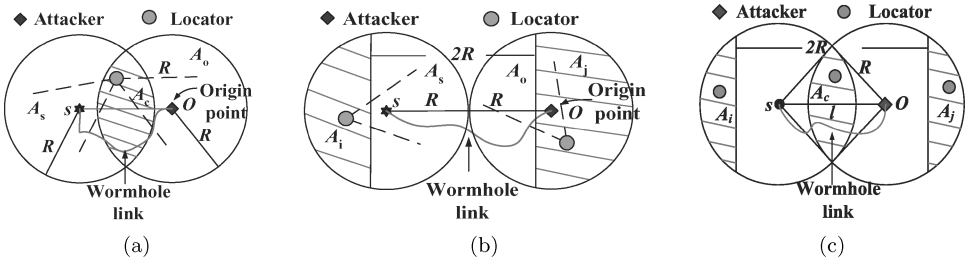

Fig. 5. (a) Single message/sector per locator property: a sensor s cannot hear two messages authenticated with the same hash value. (b) Communication range violation property: a sensor s cannot hear two locators more than $2R$ apart. (c) Combination of the two properties for wormhole detection.

The location of the sensor defines the set of locators LH_s^d directly heard to the sensor s, with $LH_s = LH_s^r \cup LH_s^d$. Based on the single message/sector per locator property we show that the wormhole attack is detected when $LH_s^r \cap LH_s^d \neq \emptyset$.

LEMMA 5.1. *Single message per locator/sector property: reception of multiple messages authenticated with the same hash value is due to replay, multipath effects, or imperfect sectorization.*

PROOF. In the absence of any attack, it is feasible for a sensor to hear multiple sectors due to multipath effects. In addition, a sensor located at the boundary of two sectors can also hear multiple sectors even if there is no multipath or attack. We assume that all sectors are transmitted simultaneously, and the same but fresh hash value is used to authenticate them per beacon transmission. Hence, sensors will only accept the first message arriving from any sector of the same locator per transmission.

Due to the use of an identical but fresh hash in all sectors per transmission, if an adversary replays a message from any sector of a locator directly heard by the sensor under attack, the sensor will have already received the hash via the direct path and, hence, detect the attack and reject the message. □

If we consider reception of multiple messages containing the same hash value due to multipath effects or imperfect sectorization to be a replay attack, a sensor will always assume it is under attack when it receives messages with the same hash value. Hence, an adversary launching a wormhole attack will always be detected if it replays a message from locator $L_i \in LH_s^d$, that is, if $LH_s^r \cap LH_s^d \neq \emptyset$. In Figure 5(a), A_s denotes the area where, $L_i \in LH_s^d$ (circle of radius R centered at s), A_o denotes the area where $L_i \in LH_s^r$ (circle of radius R centered at O), and the shaded area A_c denotes the common area $A_c = A_s \cap A_o$.

CLAIM 5.2. *The detection probability $P(SG)$ due to the single message/sector per locator property is equal to the probability that at least one locator lies within an area of size A_c, and is given by*

$$P(SG) = 1 - e^{-\rho_L A_c}, \quad \textit{with} \;\; A_c = 2R^2\phi - Rl\sin\phi, \qquad \phi = \cos^{-1}\frac{l}{2R}, \tag{8}$$

with l as the distance between the origin point and the sensor under attack.

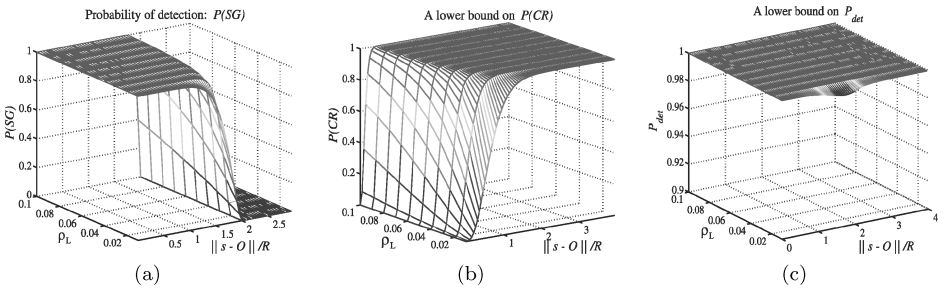

Fig. 6. Wormhole detection probability based on, (a) the single message/sector per locator property, $P(SG)$. (b) A lower bound on the wormhole detection based on the communication range violation property, $P(CR)$. (c) A lower bound on the wormhole detection probability for SeRLoc.

PROOF. If a locator L_i lies inside A_c, it is less than R units away from a sensor s and, therefore, $L_i \in LH_s^d$. Locator L_i is also less than R units away from the origin point of the attack O, and, therefore, $L_i \in LH_s^r$. Hence, if a locator lies inside A_c, $LH_s^r \cap LH_s^d \neq \emptyset$, and the attack is detected due to the single message/sector per locator property. The detection probability $P(SG)$ is equal to the probability that at least one locator lies within A_c. If LH_{A_c} denotes the set of locators located within area A_c then:

$$P(SG) = P\left(\left|LH_{A_c}\right| \geq 1\right) = 1 - P\left(\left|LH_{A_c}\right| = 0\right) = 1 - e^{-\rho_L A_c}, \tag{9}$$

where A_c can be computed from Figure 4(b) to be:

$$A_c = 2R^2\phi - Rl\sin\phi, \qquad \phi = \cos^{-1}\frac{l}{2R}, \tag{10}$$

with $l = \|s - O\|$. □

Figure 6(a) presents the detection probability $P(SG)$ vs. the locator density ρ_L and the distance $\|s - O\|$ between the origin point and the sensor under attack, normalized over R. We observe that if $\|s - O\| \geq 2R$, then $A_c = 0$, and the use of the single message/sector per locator property is not sufficient to detect a wormhole attack. For distances $\|s - O\| \geq 2R$, a wormhole attack can be detected using the following communication range constraint property.

Communication Range Violation Property. Given the coordinates of node s, all locators LH_s heard by s should lie within a circle of radius R, centered at s. Since node s is not aware of its location, it relies on its knowledge of the locator-to-sensor communication range R to verify that the set LH_s satisfies Lemma 5.3.

LEMMA 5.3. *Communication Range Constraint Property: A sensor s cannot hear two locators $L_i, L_j \in LH_s$, more than $2R$ apart, that is, $\|L_i - L_j\| \leq 2R$, $\forall L_i, L_j \in LH_s$.*

PROOF. Any locator $L_i \in LH_s$ has to lie within a circle of radius R, centered at the sensor s (area A_s in Figure 5(b)), $\|L_i - s\| \leq R, \forall L_i \in LH_s$. Hence,

$$\|L_i - L_j\| = \|L_i - s + s - L_j\| \leq \|L_i - s\| + \|s - L_j\| \leq R + R = 2R. \tag{11}$$

□

Using the coordinates of LH_s, a sensor can detect a wormhole attack if the communication range constraint property is violated. We now compute the detection probability $P(CR)$ due to the communication range constraint property.

CLAIM 5.4. *A wormhole attack is detected due to the communication range constraint property, with a probability:*

$$P(CR) \geq (1 - e^{-\rho_L A_i^*})^2, \quad A_i^* = x\sqrt{R^2 - x^2} - R^2 \tan^{-1}\left(\frac{x\sqrt{R^2 - x^2}}{x^2 - R^2}\right), \quad (12)$$

where $x = \frac{\|s-O\|}{2}$.

PROOF. Consider Figure 5(b), where $\|s-O\| = 2R$. If any two locators within A_s, A_o have a distance larger that $2R$, a wormhole attack is detected. Though $P(CR)$ is not easily computed analytically, we can obtain a lower bound on $P(CR)$ by considering the following event. In Figure 5(b), the vertical lines defining shaded areas A_i, A_j, are perpendicular to the line connecting s, O, and have a separation of $2R$. If there is at least one locator L_i in the shaded area A_i and at least one locator L_j in the shaded area A_j, then $\|L_i - L_j\| > 2R$, and the attack is detected. Note that this event does not include all possible locations of locators for which $\|L_i - L_j\| > 2R$, and hence it yields a lower bound. If $\mathcal{LH}_{A_i,A_j}$ denotes the event $(|LH_{A_i}| > 0 \cap |LH_{A_j}| > 0)$ then,

$$\begin{aligned}
P(CR) &= P(\|L_i - L_j\| > 2R, L_i, L_j \in LH_s) \\
&\geq P\left(CR \cap \mathcal{LH}_{A_i,A_j}\right) && (13)\\
&= P\left(CR \mid \mathcal{LH}_{A_i,A_j}\right) P\left(\mathcal{LH}_{A_i,A_j}\right) && (14)\\
&= P\left(\mathcal{LH}_{A_i,A_j}\right) && (15)\\
&= (1 - e^{-\rho_L A_i})(1 - e^{-\rho_L A_j}), && (16)
\end{aligned}$$

where (13) 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; (14) follows from the definition of the conditional probability; (15) follows from the fact that when $\mathcal{LH}_{A_i,A_j}$ is true, we always have a communication range constraint violation ($P(CR \mid \mathcal{LH}_{A_i,A_j}) = 1$); and (16) follows from the fact that A_i, A_j are disjoint areas and that locators are randomly deployed.

We can maximize the lower bound of $P(CR)$ by finding the optimal values A_i^*, A_j^*. In Appendix 2, we prove that the lower bound in (16) attains its maximum value when $A_i^* = \max_i\{A_i\}$, subject to the constraint $A_i = A_j$ (A_i, A_j are symmetric). We also prove that A_i^*, A_j^*, are expressed by

$$A_i^* = A_j^* = x\sqrt{R^2 - x^2} - R^2 \tan^{-1}\left(\frac{x\sqrt{R^2 - x^2}}{x^2 - R^2}\right), \quad \text{and } x = \frac{\|s - O\|}{2}. \quad (17)$$

Inserting (17) into (16) yields the required result, $P(CR) \geq (1 - e^{-\rho_L A_i^*})^2$. □

In Figure 6(b), we show the maximum lower bound on $P(CR)$ vs. the locator density ρ_L, and the distance $\|s - O\|$ normalized over R. The lower bound on $P(CR)$ 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 distances $\|s - O\| >$

$4R$ a wormhole attack is always detected based on the communication range constraint property since any locator within A_o will be more than $2R$ apart from any locator within A_s.

Detection Probability P_{det} of the Wormhole Attack Against SeRLoc. We now combine the two detection mechanisms, namely the single message/sector per locator property and the communication range constraint property for computing the detection probability of a wormhole attack against SeRLoc.

CLAIM 5.5. *The detection probability of a wormhole attack against SeRLoc is lower bounded by* $P_{det} \geq (1 - e^{-\rho_L A_c}) + (1 - e^{-\rho_L A_i^*})^2 e^{-\rho_L A_c}$.

PROOF. In the computation of the communication range constraint property, by setting $A_i = A_j$ and maximizing A_i regardless of the distance $\|s - O\|$, the areas A_i, A_j, and A_c do not overlap as shown in Figure 5(c). Hence, the corresponding events of finding a locator at any of these areas are independent and we can derive a lower bound on the detection probability P_{det} by combining the two properties.

$$\begin{aligned} P_{det} = P(SG \cup CR) &= P(SG) + P(CR) - P(SG)P(CR) \\ &= P(SG) + P(CR)(1 - P(SG)) \\ &\geq (1 - e^{-\rho_L A_c}) + (1 - e^{-\rho_L A_i^*})^2 e^{-\rho_L A_c}. \end{aligned} \tag{18}$$

The left side of (18) is a lower bound on P_{det} since $P(CR)$ was also lower bounded. □

In Figure 6(c), we show the lower bound on P_{det} vs. the locator density ρ_L and the distance $\|s - O\|$ normalized over R. For values of $\|s - O\| > 4R$, $P_{CR} = 1$ since any $L_i \in LH_s^d$ will be more than $2R$ away from any $L_j \in LH_s^r$ and hence, the wormhole attack is always detected. From Figure 6(c), we observe that a wormhole attack is detected with a probability very close to unity, independent of the origin and destination point of the attack. The intuition behind (18) is that there is at most $(1 - P_{det})$ probability for a specific realization of the network to have an origin and destination point where a wormhole attack would be successful. Even if such realization occurs, the attacker has to acquire full knowledge of the network topology and, based on the geometry, locate the origin and destination point where the wormhole link can be established.

Location Resolution Algorithm. Although a wormhole can be detected using one of the two detection mechanisms, a sensor s under attack cannot distinguish the set of locators directly heard LH_s^d from the set of locators replayed LH_s^r and hence, estimate its location. To resolve the location ambiguity sensor s executes the *Attach to Closer Locator Algorithm* (ACLA).

Assume that a sensor authenticates a set of locators $LH_s = LH_s^d \cup LH_s^r$, but detects that it is under attack.

Step 1. Sensor s broadcasts a randomly generated nonce η_s and its ID_s.

Step 2. Every locator hearing the broadcast of sensor s replies with a beacon that includes localization information and the nonce η_s, encrypted with the pairwise key $K_s^{L_i}$ instead of the broadcast key K_0. The sensor identifies the locator L_i' that replies first with an authentic message that includes η_s.

Attach to Closer Locator Algorithm (ACLA)
s : **broadcast** $\{\ \eta_s \parallel ID_s\ \}$
if L_i *hears* $\{\ \eta_s \parallel ID_s\ \}$ **reply**
L_i : $\{\ \eta_s \parallel (X_i, Y_i)\ ||\ (\theta_1, \theta_2)\ ||\ (H^{n-j}(PW_i)) \parallel j \parallel ID_{L_i}\ \}_{K_s^{L_i}}$
L_i' : *first authentic reply from a locator.*
$LH_s^d = \{L_i \in LH_s : sector\{L_i\}\ intersects\ sector\{L_i'\}\}$
s : **execute** *SeRLoc with* $LH_s = LH_s^d$

Fig. 7. The pseudocode of ACLA.

Step 3. Sensor s identifies the set LH_s^d as all the locators whose sectors overlap with the sector of L_i', and executes SeRLoc with $LH_s = LH_s^d$.

The pseudocode of ACLA is presented in Figure 7. Note that the closest locator to sensor s will always reply first if it directly hears the broadcast from s and not through a replay from an adversary. In order for an adversary to force sensor s to accept set LH_s^r as the valid locator set, it can only replay the nonce η_s to a locator $L_i \in LH_s^r$, record the reply, tunnel via the wormhole, and replay it in the vicinity of s. However, a reply from a locator in LH_s^r will arrive later than any reply from a locator in LH_s^d since locators in LH_s^r are further away from s than locators in LH_s^d.

To execute ACLA, a sensor must be able to communicate bidirectionally with at least one locator. The probability $P_{s\to L}$ of a sensor having a bidirectional link with at least one locator, and the probability P_{bd} that *all* sensors can bidirectionally communicate with at least one locator can be computed as:

$$P_{s\to L} = 1 - e^{-\rho_L \pi r^2 G^{\frac{2}{\gamma}}}, \quad P_{bd} = \left(1 - e^{-\rho_L \pi r^2 G^{\frac{2}{\gamma}}}\right)^{|S|}. \tag{19}$$

Hence, we can select the system parameters ρ_L, G so every sensor has a bidirectional link with at least one locator with any desired probability.

5.2 Sybil Attack

Threat Model. In the Sybil attack [Douceur 2002; Newsome et al. 2004], an adversary is able to fabricate legitimate node IDs or assume the IDs of existing nodes in order to impersonate multiple network entities. Unlike the wormhole attack, in the Sybil attack model, the adversary may have access to cryptographic quantities necessary to assume node IDs. Hence, the adversary can insert bogus information into the network. A solution for the Sybil attack for WSNs was recently proposed in Newsome et al. [2004].

Sybil Attack Against SeRLoc. In SeRLoc, sensors do not rely on other sensors to compute their location. Therefore, an attacker has no incentive to assume sensor IDs. An adversary can impact SeRLoc if it successfully impersonates locators. Since sensors are preloaded with valid locator IDs along with the hash values corresponding to the head of the reversed hash chain, an adversary can only duplicate existing locator IDs by compromising the globally shared key K_0.

Once K_0 has been compromised, the adversary has access to both locators IDs, the hash chain values published by the locators as well as the coordinates

of the locators. Since sensors always have the latest published hash values from the locators that they directly hear, an adversary can only impersonate locators that are not directly heard to the sensors under attack. The adversary can generate bogus beacons, attach an already published hash value from a locator not heard by the sensor under attack, and encrypt it with the compromised K_0.

Depending on the type of locators used, static or mobile, an adversary can impersonate locators in different ways. If the locators are static and their location is known before deployment, the coordinates of all locators can be preloaded to every sensor. Hence, the adversary cannot advertise a location that is different from the actual coordinates of an impersonated locator. In such a case, the Sybil attack is equivalent to a replay attack since the adversary cannot alter the content of the beacons.[3] If the locators are mobile, or their coordinates cannot be preloaded to the sensors before deployment, the adversary can place the impersonated locators to arbitrary positions. Hence, by impersonating a higher number of locators than the ones directly heard by the sensor under attack, the adversary can compromise the majority vote scheme of SeRLoc and displace the sensor.

Defense Against the Sybil Attack. Though we do not provide a mechanism to prevent an adversary from impersonating locators except for the ones directly heard by a sensor, we can still determine the position of sensors in the presence of Sybil attack. In the case where sensors know a priori the coordinates of the locators, the sensor can detect the Sybil attack with the same mechanisms used for the wormhole attack since the Sybil attack becomes a beacon replay. In the case where the coordinates of the locators are not preloaded to the sensors, an adversary can manipulate the coordinates of the impersonated locators so that neither of the wormhole defense mechanisms detect an anomaly. The adversary needs to impersonate more than LH_s^d locators in order to displace the sensor s. To avoid sensor displacement, we propose the following enhancement.

Since the locator density ρ_L is known before deployment, we can select a threshold value $L_{\max}$ as the maximum allowable number of locators heard by each sensor. If a sensor hears more than $L_{\max}$ locators, it assumes that it is under attack and executes ALCA to determine its position. The probability that a sensor s hears more than $L_{\max}$ locators is given by

$$P(|LH_s| \geq L_{\max}) = 1 - P(|LH_s| < L_{\max})) = 1 - \sum_{i=0}^{L_{\max}-1} \frac{(\rho_L \pi R^2)^i}{i!} e^{-\rho_L \pi R^2}. \quad (20)$$

Using (20), we can select the value of $L_{\max}$ so that there is a very small probability for a sensor to hear more than $L_{\max}$ locators, while there is a very high probability for a sensor to hear more than $\frac{L_{\max}}{2}$ locators. If a sensor hears more than $L_{\max}$ locators without being under attack, the detection mechanism will result in a false positive alarm and force the sensor to execute ACLA to successfully locate itself. However, if a sensor hears less than $\frac{L_{\max}}{2}$, the sensor is vulnerable to a Sybil attack. Therefore, we must select a threshold $L_{\max}$ so that any sensor hears less than $\frac{L_{\max}}{2}$ locators with a probability very close to zero.

[3]The adversary can alter the angle information contained in the beacon. However, this is equivalent to replaying the beacon of another sector.

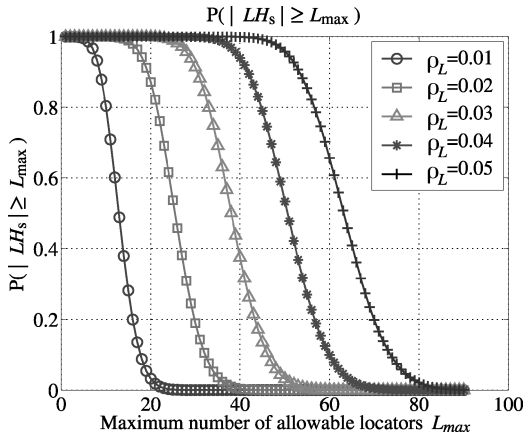

Fig. 8. $P(|LH_s| \geq L_{\max})$, vs. $L_{\max}$ for varying locator densities ρ_L.

In Figure 8, we show $P(|LH_s| \geq L_{\max})$ vs. $L_{\max}$, for varying locator densities ρ_L. Based on Figure 8, we can select the appropriate $L_{\max}$ for each value of ρ_L. For example, when $\rho_L = 0.03$, a choice of $L_{\max} = 46$ allows a sensor to localize itself when under Sybil attack with a probability $P(|LH_s| \geq 23) = 0.995$, while the false positive alarm probability is $P(|LH_s| > 46) = 0.1045$.

5.3 Compromised Network Entities

In this section, we examine the robustness of SeRLoc against compromised network entities. We consider a sensor node or a locator node to be compromised if an attacker assumes full control over the behavior of the node and knows all the keys stored at the compromised node.

Compromised Sensors. Though sensors are assumed to be easier to compromise, an attacker has no incentive to compromise sensors since they do not actively participate in the localization procedure. The only benefit in compromising a sensor is to gain access to the globally shared key K_0.

Compromised Locators. An adversary that compromises a locator L_i gains access to the globally shared key K_0, the pairwise keys $K_s^{L_i}$ that the compromised locator shares with every sensor, as well as all the hash values of the locator's hash chain. By compromising a single locator, the adversary can displace any sensor by impersonating the compromised locator from a position closer to the sensor under attack compared to the closest legitimate locator. The adversary impersonates multiple locators in order to force location ambiguity to the sensor under attack. Once the attack is detected, sensor s executes ACLA to resolve its location ambiguity. Since the adversary is closer to the sensor s than the closest legitimate locator, its reply will arrive to s first. Hence, s will assume that the impersonated set of locators is the valid one and will be displaced.

To avoid sensor displacement by a single locator compromise, we can intensify the resilience of SeRLoc to locator compromise by involving more than one locators in the location resolution algorithm at the expense of higher communication overhead. A sensor s under attack can execute the *Enhanced Location Resolution Algorithm* (*ELRA*) that follows.

Enhanced Location Resolution Algorithm (*ELRA*)
s : **broadcast** { $\eta_s \parallel LH_s \parallel ID_s$ }
$RL_s = \{L_i : \|s - L_i\| \leq r_{sL}\}$
RL_s : **broadcast** { $\eta_s \parallel LH_s \parallel ID_s \parallel (X_i, Y_i) \parallel H^{n-k}(PW_i) \parallel j \parallel ID_{L_i}$ }$_{K_0}$
$BL_s = \{L_i : \|RL_s - L_i\| \leq r_{LL}\} \bigcap LH_s$
BL_s : **broadcast** { $\eta_s \parallel (X_i, Y_i) \parallel (\theta_1, \theta_2) \parallel H^{n-k}(PW_i) \parallel j \parallel ID_{L_i}$ }$_{K_s^{L_i}}$
s : **collect** *first* $L_{\max}$ *authentic beacons from* BL_s
s : **execute** *SeRLoc with collected beacons*

Fig. 9. The pseudocode for the Enhanced Location Resolution Algorithm (ELRA).

Step 1. Sensor s broadcasts a randomly generated nonce η_s, the set of locators heard LH_s, and its ID_s.

$$s : \{\eta_s \parallel LH_s \parallel ID_s\}. \tag{21}$$

Step 2. Every locator L_i receiving the broadcast from s appends its coordinates, the next hash value of its hash chain and its ID_{L_i}, encrypts the message with K_0, and rebroadcasts the message to all sectors.

$$L_i : \{\eta_s \parallel LH_s \parallel ID_s \parallel (X_i, Y_i) \parallel H^{n-k}(PW_i) \parallel j \parallel ID_{L_i}\}_{K_0}. \tag{22}$$

Step 3. Every locator receiving the rebroadcast, verifies the authenticity of the message, and that the transmitting locator is within its range. If the verification is correct and the receiving locator belongs to LH_s, the locator broadcasts a new beacon with location information and the nonce η_s encrypted with the pairwise key with sensor s.

$$L_i : \left\{\eta_s \parallel (X_i, Y_i) \parallel (\theta_1, \theta_2) \parallel H^{n-k}(PW_i) \parallel j \parallel ID_{L_i}\right\}_{K_s^{L_i}}. \tag{23}$$

Step 4. The sensor collects the first $L_{\max}$ authentic replies from locators and executes SeRLoc with $LH_s = L_{\max}$.

The pseudocode for the enhanced location resolution algorithm is presented in Figure 9. Note that for a locator to hear the sensor's broadcast, it has to be within a range $r_{sL} = rG^{\frac{1}{\gamma}}$ from the sensor. Furthermore, in order for a the sensor to make the correct location estimate, all locators within a range R from s need to provide new beacon information.

CLAIM 5.6. *Every locator positioned within* R *from a sensor* s *is within the range of any locator positioned at a distance* r_{sL} *from the sensor* s.

PROOF. For any locator positioned at a distance r_{sL} from the sensor s to reach any locator positioned at a distance R from sensor s, the following condition has to hold: $r_{LL} \geq R + r_{sL}$. Substituting the expressions for the communication ranges from Table I.

$$RG^{\frac{2}{\gamma}} \geq R + rG^{\frac{1}{\gamma}} \Rightarrow \frac{R}{rG^{\frac{1}{\gamma}}}(G^{\frac{2}{\gamma}} - 1) \geq 1. \tag{24}$$

Since $R \geq rG^{\frac{2}{\gamma}}$ by assumption, and $G^{\frac{2}{\gamma}} \geq 1$, the left side of (24) is always greater than one. □

Each beacon broadcast from a locator has to include the nonce η_s initially broadcasted by the sensor and be encrypted with the pairwise key between the sensor and the locator. Hence, given that the sensor has at least $\frac{L_{\max}}{2}$ locators within range R with very high probability (see Figure 8), the adversary has to compromise at least $(\frac{L_{\max}}{2}+1)$ locators in order to compromise the majority vote scheme of SeRLoc. In addition, the attacker has to possess the hardware capabilities to process and transmit $(\frac{L_{\max}}{2}+1)$ replies before $\frac{L_{\max}}{2}$ replies from valid locators reach the sensor under attack. Our enhanced location resolution algorithm significantly increases the resilience of SeRLoc to locator compromise at the expense of higher communication overhead at the locators.

6. PERFORMANCE EVALUATION

In this section, we compare the performance of SeRLoc with state-of-the-art localization techniques, namely DV-Hop [Niculescu and Nath 2001], Amorphous localization [Nagpal et al. 2003], Centroid localization [Bulusu et al. 2000], APIT [He et al. 2003], and its theoretical ideal version PIT [He et al. 2003]. Based on our simulations, we show that SeRLoc has superior performance in localization accuracy and requires significantly fewer resources than other methods. Since we did not implement SeRLoc and the other localization schemes in a real environment, our results and conclusions hold for the assumptions made in the simulation. To emulate the conditions of a real deployment, we also evaluated SeRLoc under error in the locators' coordinates and false estimation of the antenna sector that includes the sensors and empirically showed that SeRLoc is robust against both sources of error.

6.1 Simulation Setup

We randomly distributed 5,000 sensors within a $100 \times 100m^2$ rectangular area. We also randomly placed locators within the same area and computed the average localization error as

$$\overline{LE} = \frac{1}{|S|}\sum_i \frac{\|\tilde{s}_i - s_i\|}{r}, \tag{25}$$

where S is the set of sensors, $\tilde{s}_i$ is the sensor estimated position, s_i is the real position, and r is the sensor-to-sensor communication range.

6.2 Localization Error vs. Locators Heard

In our first experiment, we investigated the impact of the average number of locators heard $\overline{LH}$ in the localization error. In order to provide a fair comparison of SeRLoc with other methods, we normalize $\overline{LH}$ for SeRLoc by multiplying $\overline{LH}$ with the number of sectors used. For example, when $\overline{LH}=9$, with SeRLoc using three sectors, we deployed one third of the locators for SeRLoc compared to other methods. Given the size of the deployment region $\mathcal{A}$ and the communication range R, one can compute the absolute value of the number of locators $|L|$ that need to be deployed in order to achieve a specific $\overline{LH}$ via the

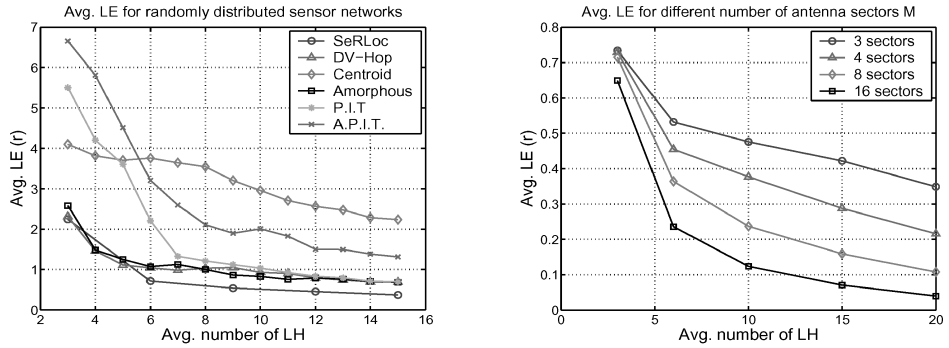

Fig. 10. (a) Average localization error $\overline{LE}$ vs. average number of locators heard $\overline{LH}$ for a network of $|N| = 5,000$ and locator-to-sensor ratio $\frac{R}{r} = 10$. (b) $\overline{LE}$ vs. $\overline{LH}$ for varying antenna sectors.

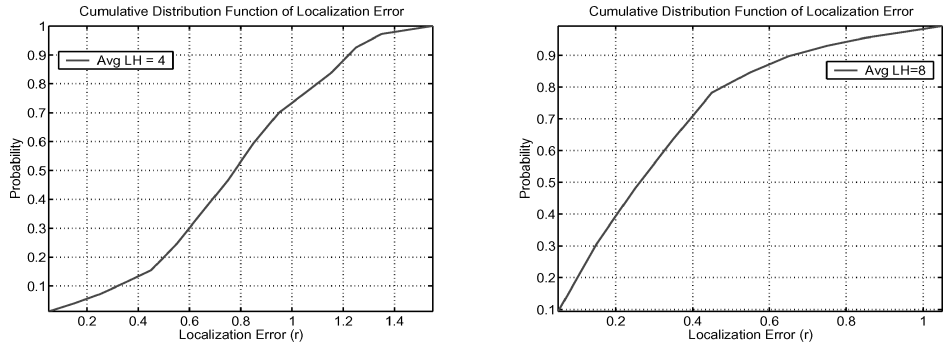

Fig. 11. The cumulative distribution function (cdf) of the localization error of SeRLoc when $M = 3$ and (a) $\overline{LE} = 4$, (b) $\overline{LH} = 8$.

formula

$$|L| = \frac{\mathcal{A}}{\pi R^2}\overline{LH}. \tag{26}$$

In Figure 10(a), we show the $\overline{LE}$ vs. $\overline{LH}$ with SeRLoc using three sectors and $\frac{R}{r} = 10$. We observe that in terms of location estimation alone, SeRLoc is superior to all other range-independent algorithms compared [Niculescu and Nath 2001; Nagpal et al. 2003; Bulusu et al. 2000; He et al. 2003]. Note that SeRLoc achieves a localization error of $0.5r$, with very few locators ($\overline{LH} = 12$ which is equivalent to four locators with 3-sectored antennas). To achieve $\overline{LE} = 0.5r$, we need a locator density of $\rho_L = \frac{4}{\pi R^2} = 0.0032$ locators/m^2 for $R = 20m$.

In Figures 11(a) and (b), we show the cumulative distribution function (cdf) of the localization error for SeRLoc when 3-sector antennas are used at the locators, and the average number of locators heard are $\overline{LH} = 6$ and $\overline{LH} = 8$, respectively. We observe that for $\overline{LH} = 4$, the error is more evenly distributed among its possible values with 90% of the sensors having an error of less than 1.2r, while for $\overline{LH} = 8$, more than 90% of the sensors have an error smaller than 0.7r.

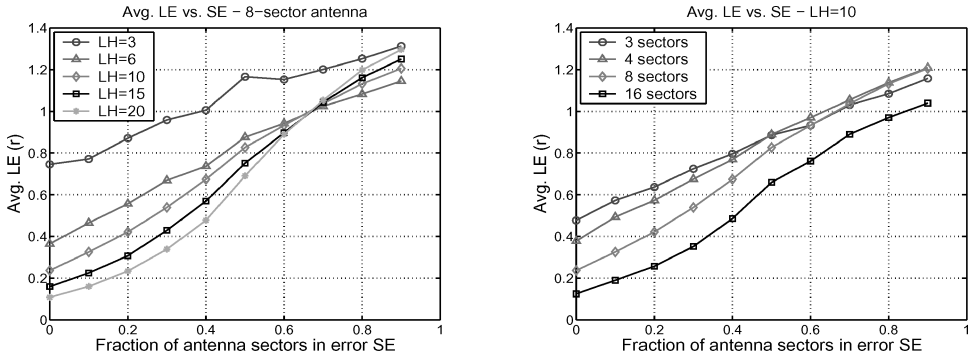

Fig. 12. (a) $\overline{LE}$ vs. sector error (SE) for varying $\overline{LH}$. (b) Average localization error $\overline{LE}$ vs. SE for a varying number of antenna sectors for a network of $|S| = 5,000$ and $\frac{R}{r} = 10$.

The highest localization error occurs when a sensor hears only one locator L_i and is R units away from L_i. The probability for such an event to occur can be set to an arbitrary small value by deploying a sufficient number of locators. For example, when $\overline{LH} = 8$, the probability for a sensor to hear just one locator is $P(|LH| = 1) = 2.7 \times 10^{-3}$.

6.3 Localization Error vs. Antenna Sectors

In our second experiment, we examined the impact of the number of antenna sectors M on the average localization error $\overline{LE}$. In Figure 10(b), we show the $\overline{LE}$ vs. $\overline{LH}$ for a varying number of antenna sectors. We can observe that for $\overline{LH} = 3$, the $\overline{LE}$ is comparable for all values of M. However, as the value of $\overline{LH}$ increases, the $\overline{LE}$ decreases more rapidly for higher number of antenna sectors due to the fact that the overlapping region becomes smaller when the antenna sectors become narrower.

The gain in the localization accuracy comes at the expense of hardware complexity at the locator since more complex antenna designs have to be employed to generate the sectoring. Additionally, errors in the estimation of the antenna sector where a sensor is included become more frequent since more sensors are located at the boundary between two sectors.

6.4 Localization Error vs. Sector Error

Sensors may be located close to the boundary of two sectors of a locator or be deployed in a region with high multipath effects. In such a case, a sensor may falsely assume that it is located in another sector than the actual sector that includes it. We refer to this phenomenon as sector error (SE) and define it as

$$SE = \frac{\text{\# of sectors falsely estimated}}{LH}. \tag{27}$$

A sector error of 0.5 indicates that *every* sensor falsely estimated the sectors of half the locators heard. In Figure 12(a), we show the $\overline{LE}$ vs. the SE for varying $\overline{LH}$ and 8-sector antennas. We observe that the $\overline{LE}$ does not grow significantly

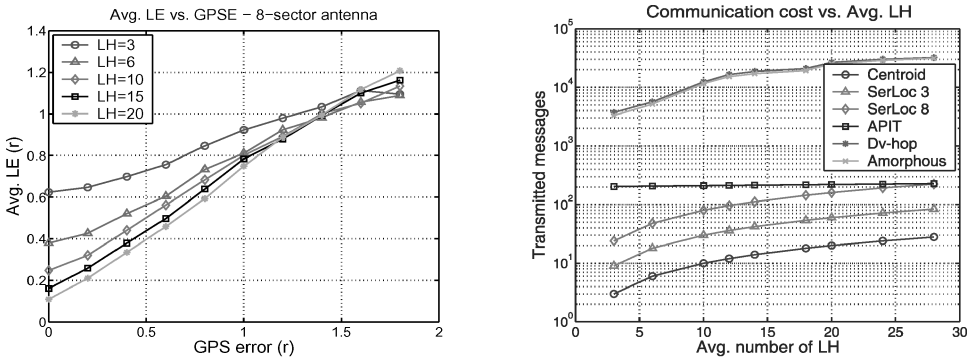

Fig. 13. (a) $\overline{LE}$ vs. locator GPS error in units of r for a varying average number of locators heard by $\overline{LH}$. (b) Communication cost vs. $\overline{LH}$ for a network of 200 sensors.

large (larger than the sensor communication range r) until a fraction of 0.7 of the sectors are falsely estimated.

SeRLoc algorithm is resilient to sector error due to the majority vote scheme employed in the determination of the overlapping region. Even if a significant fraction of sectors are falsely estimated, these sectors do not overlap in the same network area and hence a score low in the grid-sector table.

Note that for a $SE > 0.7$, $\overline{LE}$ increases with $\overline{LH}$. When the SE grows beyond a threshold, the falsely estimated sectors dominate in the location determination. As $\overline{LH}$ grows, the falsely estimated overlapping region shrinks due to the higher number of overlapping sectors. Therefore, the CoG that defines the sensor estimated location gets further apart than the actual sensor location.

In Figure 12(b), we show the $\overline{LE}$ vs. SE for $\overline{LH} = 10$ and a varying number of antenna sectors. We observe that the narrower the antenna sector, the smaller the $\overline{LE}$ even in the presence of SE. For a small SE, the overlapping region is dominated by the correctly estimated sectors and shrinks with increasing antenna sectors. For large SE, the overlapping region is dominated by the falsely estimated sectors and an increase in $\overline{LH}$ does not reduce the $\overline{LE}$.

Summarizing our findings for the sector error, we note that SeRLoc is resilient to sector error due to the majority vote mechanism employed in the overlapping region determination.

6.5 Localization Error vs. GPS Error

GPS, or any alternative localization scheme used to provide locators with their location may have limited accuracy. To study the impact of the error in the locators' position on $\overline{LH}$, we induced a GPS error ($GPSE$) to every locator of the network. A value of $GPSE = r$ means that every locator was randomly placed at a circle of radius r, centered at the locator's actual position.

In Figure 13(a), we show the average localization error $\overline{LE}$ vs. the $GPSE$ in units of r, for a varying number of $\overline{LH}$ when locators use 8-sector antennas. We observe that even for a large GPSE the $\overline{LE}$ does not grow larger than $1.2r$. For example, when $GPSE = 1.8r$ and $\overline{LH} = 3$, $\overline{LE} = 1.1r$. According to Figure 10(a),

DV-hop and amorphous localization require $\overline{LH} = 5$ to achieve the same performance in the complete absence of *GPSE*, while APIT requires $\overline{LH} = 12$ to reduce the $\overline{LE} = 1.1r$ with no GPSE induced in the locators' positions. Note that once the *GPSE* error becomes significantly large (over $1.6r$), an increase in $\overline{LH}$ does not improve the accuracy of the location estimation.

6.6 Communication Cost vs. Locators Heard

In this section, we analyse the communication cost of SeRLoc and compare it with the communication cost of the existing range-independent localization algorithms. In Figure 13(b), we show the communication cost in number of transmitted messages vs. $\overline{LH}$ when 200 sensors are randomly deployed.

We observe that DV-hop and Amorphous localization, have significantly higher communication cost compared to all other algorithms due to the flood-based approach for the beacon propagation. The centroid scheme has the lowest communication cost ($|L|$) since it only transmits one beacon from each locator to localize the sensors. APIT requires $|L| + |S|$ beacons to localize the sensors, while SeRLoc requires $M|L|$ number of beacons where L is the set of locators and M is the number of antenna sectors.

Under the assumption that the number of sensors is much higher than the number of locators, (for $|S| \gg |L|$, $|L| + |S| > M|L|$) SeRLoc has a smaller communication cost than APIT since SeRLoc is independent of the number of sensors deployed. In addition, the theoretical upper bound of the performance of APIT is given by PIT [He et al. 2003]. The APIT will achieve the performance of PIT when the sensor density ρ_s is sufficiently high. From Figure 10(a), we observe that in the simulation scenarios considered (random locator deployment), SeRLoc outperforms PIT and hence, also the APIT in average localization error for all values of $\overline{LH}$. The increased localization accuracy and lower communication cost of SeRLoc compared to other algorithms comes at the expense of more complex hardware since locators need to be equipped with sectored antennas.

7. CONCLUSION

We introduced the problem of secure localization in WSNs and proposed a range-independent, decentralized localization scheme called SeRLoc that allows sensors to determine their location in an untrusted environment. We also analytically evaluated the probability of sensor displacement due to security threats in WSNs such as the wormhole attack, the Sybil attack, and compromise of network entities and showed that SeRLoc provides accurate location estimation even in the presence of these threats. In doing so, we used the geometric and radio range information to detect the attacks on localization scheme. Our simulation studies also show that SeRLoc localizes sensors with higher accuracy than state-of-the-art range-independent localization schemes, while requiring fewer reference points and lower communication cost. Furthermore, our simulation studies showed that SeRLoc is resilient to sources of error such as location error of reference points as well as error in the sector determination. Statistical analysis and characterization of the SeRLoc estimator will be a future area of research.

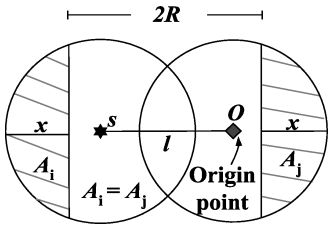

Fig. 14. Computing the maximum lower bound on $P(CR)$.

APPENDIXES

1. CHOOSING THE SYSTEM PARAMETERS

Probability of hearing more than k locators. Since locators are randomly deployed, the probability for a locator to be in an area of size A_g is $p_g = \frac{A_g}{\mathcal{A}}$. In addition, the random locator deployment implies statistical independence between locators being within a network region A_g. Hence, the probability that *exactly* k locators are in A_g is given by the binomial distribution.

$$P(k \in A_g) = \binom{|L|}{k} p_g^k (1 - p_g)^{|L|-k}. \tag{28}$$

For $|L| \gg 1$ and $\mathcal{A} \gg A_g$ we can approximate the binomial distribution with a Poisson distribution:

$$P(k \in A_g) = \frac{\frac{A_g}{\mathcal{A}}|L|}{k!} e^{-\frac{A_g}{\mathcal{A}}|L|} = \frac{\rho_L A_g}{k!} e^{-\rho_L A_g}. \tag{29}$$

By letting $A_g = \pi R^2$ we can compute the probability of having exactly k locators inside a circle of radius R, centered at the sensor.

$$P(|LH_s| = k) = \frac{(\rho_L \pi R^2)^k}{k!} e^{-\rho_L \pi R^2}. \tag{30}$$

Using (30), we compute the probability that *every* sensor hears *at least* k locators. The random sensor deployment implies statistical independence in the number of locators heard by each sensor and hence:

$$P(|LH_s| \geq k, \forall\, s) = (1 - P(|LH_s| < k))^{|S|} = \left(1 - \sum_{i=0}^{k-1} \frac{(\rho_L \pi R^2)^i}{i!} e^{-\rho_L \pi R^2}\right)^{|S|}. \tag{31}$$

2. MAXIMIZING THE LOWER BOUND ON $P(CR)$

The lower bound on detection probability based on the communication range constraint property is given by

$$P(CR) \geq (1 - e^{-\rho_L A_i})(1 - e^{-\rho_L A_j}). \tag{32}$$

We want to compute the values of A_i^*, A_j^* that maximize the right side of (32). From Figure 14,

$$A_i(x) = 2\int_{R-x}^{R}\sqrt{R^2-z^2}dz, \qquad A_j(x) = 2\int_{R+x-l}^{R}\sqrt{R^2-z^2}dz, \tag{33}$$

where $l = \|s - O\|$. Since, both A_i, A_j are expressed as function of x, the lower bound $LB(x)$ on $P(CR)$ can be expressed as

$$LB(x) = (1 - e^{-\rho_L A_i(x)})(1 - e^{-\rho_L A_j(x)}). \tag{34}$$

To maximize $LB(x)$, we differentiate over x and set the derivative equal to zero:

$$\begin{aligned} LB'(x) &= \rho_L A_i'(x)e^{-\rho_L A_i(x)} + \rho_L A_j'(x)e^{-\rho_L A_j(x)} \\ &\quad - \rho_L(A_i'(x) + A_j'(x))e^{-\rho_L(A_i(x)+A_j(x))} \\ &= \rho_L A_i'(x)\left(e^{-\rho_L A_i(x)} - e^{-\rho_L(A_i(x)+A_j(x))}\right) \\ &\quad + \rho_L A_j'(x)\left(e^{-\rho_L A_j(x)} - e^{-\rho_L(A_i(x)+A_j(x))}\right) = 0. \end{aligned} \tag{35}$$

A trivial solution to $LB'(x) = 0$ is $A_i(x) = 0$, or $A_j(x) = 0$, but both yield a minimum rather than a maximum ($LB(x) = 0$). However if we set $A_i(x) = A_j(x)$, from (33), we obtain $R + x - l = R - x \Rightarrow x = \frac{l}{2}$. In addition, differentiating (33) with respect to x and evaluating (33) at $x = \frac{l}{2}$ yields $A_i'(\frac{l}{2}) = -A_j'(\frac{l}{2})$. Hence, for $A_i(x) = A_j(x)$, $LB'(x) = 0$, and the maximum value on the lower bound $LB(x)$ is achieved. The values of A_i, A_j that maximize $LB(x)$ are

$$A_i^*(x) = 2\int_{R-x}^{R}\sqrt{R^2-z^2}dz = x\sqrt{R^2-x^2} - R^2\tan^{-1}\left(\frac{x\sqrt{R^2-x^2}}{x^2-R^2}\right). \tag{36}$$

ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

BASAGNI, S., CHLAMTAC, I., SYROTIUK, V., AND WOODWARD, B. 1998. A distance routing effect algorithm for mobility (dream). In *Proceedings of MOBICOM'98*. 76–84.

BULUSU, N. 2002. Self-configuring localization systems. PhD thesis, UCLA.

BULUSU, N., HEIDEMANN, J., AND ESTRIN, D. 2000. Gps-less low cost outdoor localization for very small devices. *IEEE Person. Comm. Mag. 7*, 5 (Oct.), 28–34.

CAMP, T., BOLENG, J., AND DAVIES, V. 2002. A survey of mobility models for ad hoc network research. *Wirel. Comm. Mobile Comput. (WCMC): Special Issue on Mobile Ad Hoc Networking:Research, Trends and Applications*, 483–502.

ČAPKUN, S., HAMDI, M., AND HUBAUX, J. 2001. Gps-free positioning in mobile ad-hoc networks. In *Proceedings of Hawaii International Conference on System Sciences (HICCSS'01)*. 3481–3490.

ČAPKUN, S. AND HUBAUX, J. 2005. Secure positioning of wireless devices with application to sensor networks. *To appear in Proceedings of Infocom'05*.

COPPERSMITH, D. AND JAKOBSSON, M. 2002. Almost optimal hash sequence traversal. In *Proceedings of the Financial Cryptography 6th International Conference (FC'02)* Lecture Notes in Computer Science. Vol. 2357. 102–119.

CRESSIE, N. 1993. *Statistics for Spatial Data*. John Wiley & Sons, New York, NY.

DOHERTY, L., GHAOUI, L., AND PISTER, K. 2001. Convex position estimation in wireless sensor networks. In *Proceedings of the IEEE INFOCOM'01*. Vol. 3. 1655–1663.

DOUCEUR, J. 2002. The sybil attack. In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02)* Lecture Notes in Computer Science. Vol. 2429. 251–260.

GRUTESER, M., SCHELLE, G., JAIN, A., HAN, R., AND GRUNWALD, D. 2003. Privacy-aware location sensor networks. In *Proceedings of the 9th Workshop on Hot Topics in Operating Systems (HotOS'03)*.

HE, T., HUANG, C., BLUM, B., STANKOVIC, J., AND ABDELZAHER, T. 2003. Range-free localization schemes in large scale sensor network. In *Proceedings of ACM MOBICOM'03*. 81–95.

HOFMANN-WELLENHOF, B., LICHTENEGGER, H., AND COLLINS, J. 1997. *Global Positioning System: Theory and Practice*. Springer-Verlag.

HU, Y., PERRIG, A., AND JOHNSON, D. 2003. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proceedings of INFOCOM'03*. 1976–1986.

KARLOF, C., SASTRY, N., AND WAGNER, D. 2004. Tinysec: A link layer security architecture for wireless sensor networks. In *Proceedings of SenSys'04*. 162–175.

KARLOF, C. AND WAGNER, D. 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad-Hoc Networks 1*, 293–315.

KLEINROCK, L. AND SLIVESTER, J. 1978. Optimum transmission radii for packet radio networks or why six is a magic number. In *Proceedings of the National Telecom Conference*. 4.3.1–4.3.5.

LAMPORT, L. 1981. Password authentication with insecure communication. *Comm. ACM 24*, 11 (Nov.), 770–772.

LAZOS, L. AND POOVENDRAN, R. 2003. Energy-aware secure multicast communication in ad-hoc networks using geographic location information. In *Proceedings of International Conference on Acoustics, Speech and Signal Processing (ICASSP'03)*. Vol. 6. 201–204.

LAZOS, L. AND POOVENDRAN, R. 2004. SeRLoc: Secure range-independent localization for wireless sensor networks. In *Proceedings of ACM Workshop on Wireless Security (WISE'04)*. 21–30.

MICA. Mica wireless measurement system. Available at http://www.xbow.com/Products/Product_pdf_files /Wireless_pdf/MICA.pdf.

NAGPAL, R., SHROBE, H., AND BACHRACH, J. 2003. Organizing a global coordinate system from local information on an ad hoc sensor network. In *Proceedings of Information Processing in Sensor Networks (IPSN'03)* Lecture Notes in Computer Science. Vol. 2634. 333–348.

NEWSOME, J., SHI, E., SONG, D., AND PERRIG, A. 2004. The sybil attack in sensor networks: Analysis and defenses. In *Proceedings of Information Processing in Sensor Networks (IPSN'04)*. 259–268.

NICULESCU, D. AND NATH, B. 2001. Ad-hoc positioning systems (aps). In *Proceedings of IEEE GLOBECOM'01*. Vol. 5. 2926–2931.

NICULESCU, D. AND NATH, B. 2003. Ad hoc positioning system (aps) using aoa. In *Proceedings of INFOCOM'03*. Vol. 3. 1734–1743.

PAPADIMITRATOS, P. AND HAAS, Z. J. 2002. Secure routing for mobile ad hoc networks. In *Proceedings of the Center for Networking and Distributed Systems (CNDS'02)*.

PICKHOLTZ, R., SCHILLING, D., AND MILSTEIN, L. 1982. Theory of spread spectrum communications—A tutorial. *IEEE Trans. Comm. 30*, 5 (May), 855–884.

PRIYANTHA, N., BALAKRISHNAN, H., DEMAINE, E., AND TELLER, S. 2003. Anchor-free distributed localization in sensor networks. In *Proceedings of ACM SenSys'03*. 340–341.

RAMANATHAN, R. 2001. On the performance of ad hoc networks with beamforming antennas. In *Proceedings of MobiHoc'01*. 95–105.

RIVEST, R. 1995. The rc5 encryption algorithm. In *Proceedings of the 1st Workshop on Fast Software Encryption*. 86–96.

SASTRY, N., SHANKAR, U., AND WAGNER, D. 2002. Secure verification of location claims. In *Proceedings of ACM Workshop on Wireless Security (WISE'02)*. 1–10.

SAVVIDES, A., HAN, C., AND SRIVASTAVA, M. 2001. Dynamic fine-grained localization in ad-hoc networks of sensors. In *Proceedings of ACM MOBICOM'01*. 166–179.

SHANG, Y., RUML, W., ZHANG, Y., AND FROMHERZ, M. 2003. Localization from mere connectivity. In *Proceedings of MOBIHOC'03*. 201–212.

STINSON, D. 2002. *Cryptography: Theory and Practice*. CRC Press.

WICKER, S. AND BARTZ, M. 1994. Type-ii hybrid-arq protocols using punctured mds codes. *IEEE Trans. Comm. 42*, 2/3/4, 1431–1440.

YAZDI, N., AYAZI, F., AND NAJAFI, K. 1998. Micromachined inertial sensors. In *Proceedings of the IEEE*. Vol. 85, 8 (Aug.), 1640–1659.

Received September 2004; revised January 2005; accepted May 2005