HiRLoc: High-resolution Robust Localization for Wireless Sensor Networks

Loukas Lazos and Radha Poovendran
Network Security Lab, Dept. of EE,
University of Washington, Seattle, WA 98195-2500
{l_lazos, radha}@ee.washington.edu

***Abstract*— In this paper we address the problem of robustly estimating the position of randomly deployed nodes of a Wireless Sensor Network (WSN), in the presence of security threats. We propose a range-independent localization algorithm called HiRLoc, that allows sensors to passively determine their location with high resolution, without increasing the number of reference points, or the complexity of the hardware of each reference point. In HiRLoc, sensors determine their location based on the intersection of the areas covered by the beacons transmitted by multiple reference points. By combining the communication range constraints imposed by the physical medium with computationally efficient cryptographic primitives that secure the beacon transmissions, we show that HiRLoc is robust against known attacks on WSN, such as the wormhole attack, the Sybil attack and compromise of network entities. Finally, our performance evaluation shows that HiRLoc leads to a significant improvement in localization accuracy compared to state-of-the-art range-independent localization schemes, while requiring fewer reference points.**

***Index Terms*— Algorithm, Design, Performance, Security**

I. Introduction

When wireless sensor networks (WSN) are deployed to monitor and record a wide range of valuable information, such as acoustic, visual, thermal, seismic, or any other type of measured observation, it is essential that sensor reports are coupled with the location that the observation occurred. Since future applications of WSN envision on-demand network deployment in a self-configurable way with no pre-specified structure or supporting infrastructure, sensors cannot know their location apriori. Hence, sensors need to apply a localization process in order to discover their location. This localization process must occur during the network initialization and when the location of the sensor changes, or, alternatively, can be applied on demand when localization information is required by network protocols such as, routing and security protocols [2], [12], [17].

Since sensors are intended to be low-cost disposable devices, currently developed solutions such as GPS [11], are inadequate for the hardware and power-limited sensors. Furthermore, since WSN may be deployed in hostile environments and operate in an untethered manner, they are susceptible to a variety of attacks [9], [12], [14] that could significantly impact the accuracy of the localization process. Since location information is an integral part of most wireless sensor network services such as geographical routing [2], and applications such as target tracking and monitoring, it is of paramount importance to secure the localization process. While the topic of sensor localization in a trusted environment has been extensively studied in the literature, [1], [5], [10], [25], [26], [30], [31], localization in the presence of malicious adversaries remains an unexplored area of research [6], [15], [18]–[22].

In this paper we address the problem of *enabling nodes of a WSN to compute a high-resolution estimate of their location even in the presence of malicious adversaries.* This problem will be referred to as *High Resolution Secure Localization*. Since sensors are limited in hardware capabilities we pursue solutions that do not require any special ranging hardware at the sensor side to infer quantities such as range or angle of arrival estimates. We refer to those solutions as range-independent. Specifically, we consider secure localization for wireless sensor networks in the context of, (a) decentralized and scalable implementation, (b) resource efficiency in computation, communication and storage, (c) range-independence, and (d) robustness against security threats in WSN.

In this paper we make the following contributions. We introduce a novel localization scheme for WSN called High-resolution Range-independent Localization (HiRLoc), that allows sensors to passively determine their location with high accuracy (sensors do not interact to determine their location). The increased localization accuracy is the result of combination of multiple localization information over a short time period, and does not come at the expense of increased hardware complexity or deployment of reference points with higher density. Since our method does not perform any range measurements to estimate the sensors' location, it is not susceptible to any range measurement alteration attacks. Furthermore, sensors do not rely on other sensors to infer their location and hence, the robustness of our localization method does not rely on the easily tampered sensor devices. Finally, we show that our method is robust against well known security threats in WSN, such as the wormhole attack [12], [28], the Sybil attack [9], [13], [33], and compromise of network entities. Based on our performance evaluation, we show that HiRLoc localizes sensors with higher resolution than previously proposed decentralized range-independent localization schemes [3], [10], [18], [25], [26], while requiring fewer hardware resources.

The remainder of the paper is organized as follows: In Section II we state our network model assumptions. Section III describes HiRLoc and Section IV presents the security analysis. In Section V, we provide the performance evaluation. In Section VI we review related work and in Section VII we present open problems and discussion. Section VIII presents our conclusions.

II. Network Model Assumptions

Network deployment: We assume that a set of sensors S with *unknown location* is randomly deployed with a density ρ_s within an area $\mathcal{A}$. We also assume that a set of specially equipped nodes with *known location*[1] and orientation, called locators are also randomly deployed with a density ρ_L, with $\rho_s \gg \rho_L$.

The random deployment of the locators with a density ρ_L can be modeled after a *homogeneous Poisson point process* of rate ρ_L [8]. The random deployment of sensors with a density ρ_s, can be modeled after a random sampling of the area $\mathcal{A}$ with rate ρ_s [8]. If LH_s denotes the set of locators heard by a sensor s, i.e. being within range R from s, the probability that s hears exactly k locators, is given by the Poisson distribution [8]:

$$P(|LH_s| = k) = \frac{(\rho_L \pi R^2)^k}{k!} e^{-\rho_L \pi R^2}. \tag{1}$$

Note that (1) provides the probability that a randomly chosen sensor hears k locators given that locators are randomly distributed and not Poisson distributed [8].

Antenna model: We assume that sensors are equipped with omnidirectional antennas, able to transmit with maximum power P_s, while locators are equipped with M directional antennas with a directivity gain $G > 1$, and can simultaneously transmit on each antenna with maximum power $P_L > P_s$.[2] We also assume that locators can vary their transmission range from zero to a maximum value of R, via power control. Furthermore, we assume that locators can change their antenna direction, either through changing their orientation or rotating their directional antennas.

III. HiRLoc: High-resolution Range-Independent Localization Scheme

In this section we present the High-resolution Range-independent Localization scheme (*HiRLoc*) that allows sensors to determine their location with high accuracy even in the presence of security threats. HiRLoc achieves passive sensor localization based on beacon information transmitted from the locators with improved resolution compared to our initial algorithm (SeRLoc) presented in [18], [19], at the expense of increased computational complexity and communication.

A. Location Determination

In order to determine their location, sensors rely on beacon information transmitted from the locators. Each locator transmits a beacon at each directional antenna that contains, (a) the locator's coordinates, (b) the angles of the sector boundary lines defined by the directional transmission, with respect to a common global axis and, (c) the locator's communication range R. Locators may change their orientation over time and retransmit beacons in order to improve the accuracy of the location estimate. Based on the beacon information, sensors define the sector area $S_i(j)$ as the confined area covered by the j^{th} transmission of a locator L_i.

A sensor s receiving the j^{th} beacon transmission from locator L_i, is included within the sector area $S_i(j)$. Note that sensors do not perform any signal strength, time of flight, or angle of arrival measurement and hence, HiRLoc is a range-independent localization scheme. Let $LH_s(j)$ denote the set of locators heard by a sensor s, during the j^{th} transmission round. By collecting beacons from the locators $L_i \in LH_s(j)$, the sensor can compute its location (an area rather than a single point), as the *Region of Intersection* (ROI) of all the sectors $S_i(j)$. Note that a sensor can hear beacons from multiple locators, or multiple beacons generated by the same locator. Hence, the ROI after the m^{th} round of beacon transmissions can be expressed as the intersection of all the sectors corresponding to the beacons available at each sensor:

$$ROI(m) = \bigcap_{j=0}^{m} \left(\bigcap_{i=1}^{|LH_s(j)|} S_i(j) \right). \tag{2}$$

Since the ROI indicates the confined region where the sensor is located, reducing the size of the ROI leads to an increase in the localization accuracy. Based on equation (2), we can reduce the size of the ROI by, (a) reducing the size of the sector areas $S_i(j)$ and, (b) increase the number of intersecting sectors $S_i(j)$.

In our previous algorithm named SeRLoc [18], [19], sensors compute their location by collecting only one beacon transmission from each locator. Since subsequent rounds of transmissions contain identical sector information as the first round of transmissions, the reduction of the ROI in SeRLoc can only be achieved by, (a) increasing the locator density ρ_L so that more locators are heard at each sensor, and higher number of sectors intersect or, (b) by using narrower antenna sectors to reduce the size of the sectors $S_i(j)$. Both these methods reduce the localization error at the expense of higher number of devices with special capabilities (more locators), and more complex hardware at each locator (more antenna sectors).

In HiRLoc, we propose methods for reducing the ROI by exploiting the temporal dimension, and without incurring the costs of deploying more locators, or equipping them with expensive antenna systems. The locators provide different localization information at consecutive beacon transmissions by, (a) varying the direction of their antennas and, (b) varying the communication range of the transmission via power control. We now explore how both these methods lead to the reduction of the ROI.

1. Varying the antenna orientation: The locators are capable of transmitting at all directions (omnidirectional coverage) using multiple directional antennas. Every antenna has a

[1] Position can be acquired through manual insertion or through GPS receivers [11]. Though GPS signals can be spoofed, knowledge of the coordinates of several nodes is essential to generate a coordinate reference system. An effort to secure GPS localization has been recently proposed in [15].

[2] The higher transmission power at the locators is a reasonable assumption, given that sensors are low-power devices. A typical sensor has a maximum transmission power of $P_s = 0.75mW$ [24]. For a homogeneous medium with attenuation factor $\gamma = 2$ locators need to transmit with a power $P_g = 75mW$ to achieve a communication range ratio $\frac{R}{r} = 10$, without taking into consideration the directivity gain of the locators' antennas.

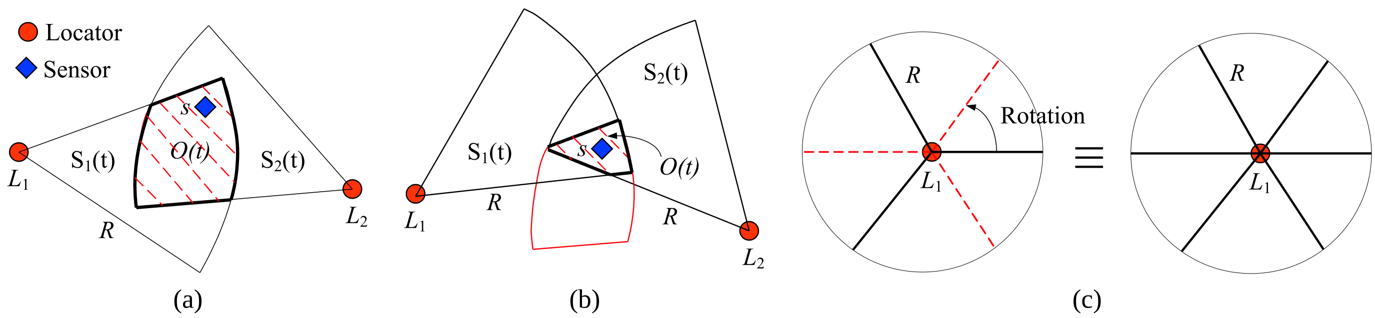


Fig. 1. (a) The sensor is located within the intersection of the sectors $S_1(j), S_2(j)$, which defines the region of intersection ROI. (b) The ROI is reduced by the rotation of the antenna sectors by some angle α. (c) Locator L_1 is equipped with three directional antennas of beamwidth $\frac{2\pi}{3}$ each. The transmission of beacons at each sector, followed by antenna rotation by $\frac{\pi}{3}$, followed by a transmission of update beacons, is equivalent to equipping L_1 with six directional antennas of beamwidth $\frac{\pi}{3}$.

specific orientation and hence corresponds to a fixed sector area $S_i(j)$. The antenna orientation is expressed by the angle information contained in the beacon $\theta_i(j) = \{\theta_{i,1}(j), \theta_{i,2}(j)\}$, where $\theta_{i,1}(j), \theta_{i,2}(j)$ denote the lower and upper bounds of the sector $S_i(j)$.

Instead of reducing the size of the intersecting sectors by narrowing the antenna beamwidth, locators can change the orientation of their antennas and re-transmit beacons with the new sector boundaries. A change in the antenna orientation can occur either by changing the orientation of the locators, or by rotation of their antenna system. A sensor collects multiple sector information from each locator over a sequence of transmissions: $S_i(j) = S_i(\theta_i(j), j), j = 1 \ldots Q$. As expressed by equation (2), the intersection of a larger number of sectors can lead to a reduction in the size of the ROI. As an example, consider figure 1 where a sensor s hears locators L_1, L_2. In figure 1(a), we show the first round of beacon transmissions by the locators L_1, L_2, and the corresponding $ROI(1)$. In figure 1(b), the locators L_1, L_2 rotate their antennas by an angle α and transmit the second round of beacons with the new sector boundaries.The ROI in the two rounds of beacon transmissions, can be expressed as:

$$\begin{aligned} ROI(1) &= S_1(1) \cap S_2(1), \\ ROI(2) &= S_1(1) \cap S_1(2) \cap S_2(1) \cap S_2(2). \end{aligned} \quad (3)$$

The antenna rotation can be interpreted as an increase on the number of antenna sectors of each locator via superposition over time. For example, consider figure 1(c), where a locator is equipped with three directional antennas of beamwidth $\frac{2\pi}{3}$. Transmission of one round of beacons, followed by antenna rotation by $\frac{\pi}{3}$ and re-transmission of the updated beacons is equivalent to transmitting one round of beacons when locators are equipped with six directional antennas of beamwidth $\frac{\pi}{3}$.

2. Varying the Communication range: A second approach to reduce the area of the ROI, is to reduce the size of the intersecting sectors. This can be achieved by allowing locators to decrease their transmission power and re-broadcast beacons with the new communication range information. In such a case, the sector area $S_i(j)$ is dependent upon the communication range $R_i(j)$ at the j^{th} transmission, i.e. $S_i(j) = S_i(R(j), j)$. To illustrate the ROI reduction, consider figure 2(a), where locators L_1, L_2 transmit with their maximum power; sensor s computes: $ROI(1) = S_1(1) \cap S_2(1)$. In figure 2(b), locators L_1, L_2 reduce their communication range by lowering their transmission power and re-transmit the updated beacons. While locator L_1 is out of range from sensor s and, hence, does not further refine the sensor's location, s can still hear locator L_2 and therefore, reduce the size of the ROI.

3. Hybrid approach: The combination of the variation of the antenna orientation and communication range leads to a dual dependency of the sector area $S_i(\theta_i(j), R(j), j)$. Such a dependency can also be interpreted as a limited mobility model for the locators. For a locator L_i moving in a confined area, the antenna orientation and communication range with respect to a static sensor varies, thus providing the sensor with multiple sector areas $S_i(j)$. The mobility model is characterized as limited, since the locator has to be within the range of the sensor for at least a fraction of its transmissions in order to provide the necessary localization information. We now present the algorithmic details of HiRLoc.

B. *The algorithmic details of HiRLoc*

Equation (2), expresses two different ways of computing the region of intersection. We can, (a) collect all beacons over several transmission rounds and compute the intersection of the all sector areas or, (b) estimate ROI after every round of transmissions and intersect it with the previous estimate of the ROI. We will refer to the first approach as HiRLoc-I and the latter approach as HiRLoc-II. Though both of these approaches result in the same estimate of the ROI, they exhibit different properties explained below.

HiRLoc-I: *Computing the intersection of all sector areas*

In the first version of HiRLoc the estimation of the ROI is computed by collecting all beacons transmitted by each locator over time, intersecting all sectors of each locator and then intersecting the outcome.

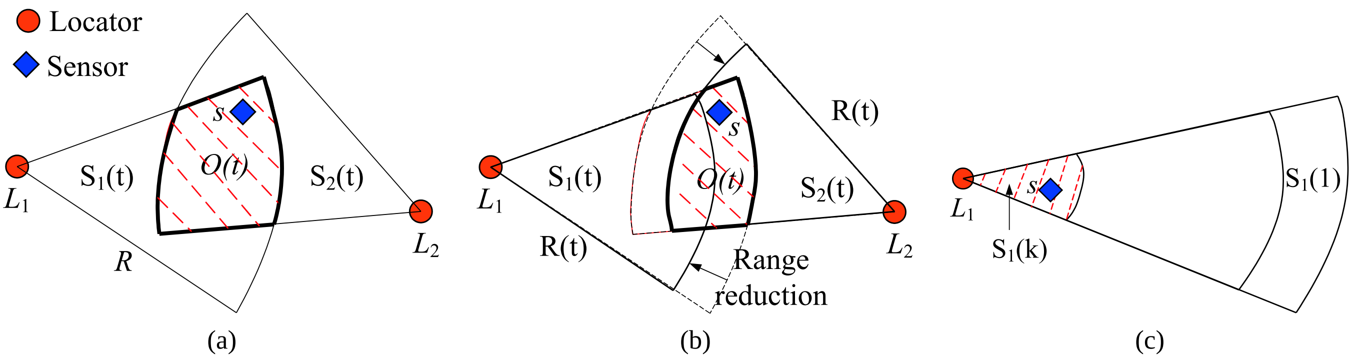


Fig. 2. (a) The sensor is located within the intersection of the sectors $S_1(j), S_2(j)$, which defines the ROI, (b) the locators reduce their communication range and transmit updated beacons. While s is outside the communication range of L_1, it can still hear the transmission of L_2. The new beacon information leads to the reduction of the ROI. (c) The intersection of multiple sectors originating from the same locator with the same angle boundaries but different transmission range $R_i(j)$ is equal to the sector with the smallest communication range.

$$ROI(m) = \bigcap_{|LH_s|} \left(\bigcap_{j=0}^{m} S_i(j) \right) \tag{4}$$

The algorithmic steps performed are:

Step 1: **Initial estimate of the ROI**—In step 1, the sensor determines the set of locators LH_s that will be used for its localization. Based on the coordinates of the locators $L_i \in LH_s$, and the maximum communication range of the locators, denoted as R_{max}, the sensor calculates the first estimate of the ROI as follows: Let $X_{min}, Y_{min}, X_{max}, Y_{max}$ denote the minimum and maximum locator coordinates form the set LH_s defined as:

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

Since every locator in set LH_s is within a range R_{max} from sensor s, if s can hear locator L_i with coordinates (X_{min}, Y_i), it has to be located *left* from the vertical boundary of ($X_{min} + R$). Similarly, s has to be located *right* from the vertical boundary of ($X_{max} - R$), *below* the horizontal boundary of ($Y_{min} + R$), and *above* the horizontal boundary of ($Y_{max} - R$).

Step 2: **Beacon collection**—In step 2, sensors continue to collect all the beacons heard over multiple beacon transmission rounds[3], generated due to changes in the parameters of the antenna sector. We describe three different options on the type of parameter changes that the locators can perform.

Option A: Antenna orientation variation—The locators rotate their antennas by a pre-specified angle $\alpha = \frac{2\pi}{QM}$, where M is the number of antenna sectors at each locator and $(Q-1)$ is the total number of antenna rotations until the initial configuration is repeated (A total of Q different transmissions take place). The antenna orientation variation increases the number of sectors defining the ROI by a factor of $(Q-1)$. The number of intersecting sector $S_i(j)$ is equal to $Q|LH_s|$. Hence, the algorithmic complexity for computing the ROI is increased by a factor of $(Q-1)$ compared to SeRLoc [18].

[3]The j^{th} transmission round is defined as the time until every locator $L_i \in LH_s$ has completed its j^{th} beacon transmission.

Option B: Communication range variation—The locators reduce their communication range by a pre-specified amount at each transmission round. If N is the total number of distinct communication ranges, the locators reduce the range by $\frac{R_{max}}{N}$, at each round.

Note that not all beacons from the same locator provide useful information for the determination of the ROI. As an example, consider figure 2(c) where the locator L_1 gradually reduces its transmission range from R_{max} to $\frac{(N-k)R_{max}}{N}$. Since $\cap_{j=1}^{k} S_i(j) = S_i(k)$, if a sensor is able to hear the k^{th} transmission of L_1, only the sector area corresponding to $S_i(k)$ contributes to the estimation of the ROI. Hence, all previous beacons can be ignored. The communication range variation does not increase the number intersecting areas and hence does not increase the algorithmic complexity compared to SeRLoc [18]. The number of sector areas that intersect to define the ROI is equal to $|LH_s|$.

Option C: Combination of options A, B—Locators can variate both their communication range and their antenna orientation, by going through a total of $(Q-1)(N-1)$ steps. The number of sectors $S_i(j)$ that intersect to define the ROI is $(Q-1)|LH_s|$, and the algorithmic complexity is equal to option A.

Step 3: **Determination of the ROI**—Though analytical computation of the ROI is achievable based on the intersection of the boundary lines of the sectors, in order to reduce the computational complexity, each sensor uses a majority vote-based scheme as in SeRLoc [18], and described briefly here. The sensor places a grid of equally spaced points within the first estimate of the ROI computed in Step 1. For each grid point, the sensor holds a score in a Grid Score Table (GST), with initial scores set to zero. Let g_i denote the i^{th} grid point.

HiRLoc-I: High-resolution Robust Localization Scheme

L_i : **broadcast** $\{ (X_i, Y_i) \mid\mid (\theta_{i,1}(1), \theta_{i,2}(1)) \mid\mid R_i(1)\}$
s : **define** $LH_s = \{L_i : \|s - L_i\| \leq R_i(1)\}$
s : **define** $A_s = [X_{max} - R_i(1),\ X_{min} + R_i(1),$
$Y_{max} - R_i(1),\ Y_{min} + R_i(1)]$
s : **store** $S \leftarrow S_i(1) :\ \{ (X_i, Y_i) \mid\mid (\theta_{i,1}(1), \theta_{i,2}(1)) \mid\mid R_i(1)\},$
$\forall L_i \in LH_s$
$j = 1$
for $k = 1 : Q - 1$
for $w = 1 : N - 1$
$j + +$
L **reduce** $R(j) = R(j-1) - \frac{R(1)}{N}$
L : **broadcast** $\{ (X_i, Y_i) \mid\mid (\theta_{i,1}(j), \theta_{i,2}(j)) \mid\mid R_i(j)\}$
$s : S \leftarrow S_i(j) :\ \{ (X_i, Y_i) \mid\mid (\theta_{i,1}(j), \theta_{i,2}(j)) \mid\mid R_i(j)\},$
$\forall L_i : \|s - L_i\| \leq R_i(j) \bigcap L_i \in LH_s$
endfor
$j + +$
$R_i(j) = R_i(1), \quad \forall L_i \in LH_s$
L **rotate** $\theta_i(j) = \{\theta_{i,1}(j-1) + \frac{2\pi}{MQ}, \theta_{i,2}(j-1) + \frac{2\pi}{MQ}\}$
L : **broadcast** $L_i :\ \{ (X_i, Y_i) \mid\mid (\theta_{i,1}(j), \theta_{i,2}(j)) \mid\mid R_i(j)\}$
s : **store** $S \leftarrow S_i(j) :\ \{ (X_i, Y_i) \mid\mid (\theta_1(j), \theta_2(j)) \mid\mid R_i(j)\},$
$\forall L_i : \|s - L_i\| \leq R(j) \bigcap L_i \in LH_s$
endfor
s : **compute** $ROI = \bigcap_{i=1}^{|S|} S_i$

Fig. 3. The pseudo-code for the High-resolution Robust Localization algorithm (version I).

For each grid point g_k the sensor *increases* the corresponding score in the grid score table with respect to a sector $S_i(j)$ corresponding to a locator $L_i \in LH_s$ if the two following conditions are satisfied:

$$C_1 :\ \ \|g_k - L_i\| \leq R_i(j), \quad C_2 :\ \theta_{i,1}(j) \leq \phi \leq \theta_{i,2}(j), \quad (6)$$

where ϕ is the slope of the line connecting g_k with L_i. The sensor determines the ROI as the grid points with the highest score on the grid score table:

$$ROI = \{g_{i^*} : i^* = \arg\max_i GST(i)\}. \quad (7)$$

HiRLoc-II: *Computing the sector intersection at each transmission round*

In our second approach, the sensor computes the ROI by intersecting all collected information at each transmission round.

$$ROI(m) = \bigcap_{j=0}^{m} \left(\bigcap_{i=1}^{|LH_s(j)|} S_i(j) \right). \quad (8)$$

At a transmission round m the sensor intersects the newly acquired sectors as described in step 3 of HiRLoc-I, and computes ROI_m :

$$ROI_m = \bigcap_{i=1}^{|LH_s(m)|} S_i(m). \quad (9)$$

Then, the sensor intersects the ROI_m with the previous estimate $ROI(m-1)$ to acquire the current estimate.

$$ROI(m) = ROI_m \bigcap ROI(m-1) = \bigcap_{j=1}^{m} \left(\bigcap_{i=1}^{|LH_s(j)|} S_i(j) \right) \quad (10)$$

HiRLoc-II can be seen as an iterative application of SeRLoc [18], with sensors using SeRLoc at each transmission round to estimate ROI_t and intersecting it with the previous one.

Comparison of HiRLoc-I and HiRLoc-II: Though both versions of HiRLoc result in the same ROI estimation once all transmission rounds have been completed, the two methods have different algorithmic complexity. In HiRLoc-I we make use of a smaller number of sectors compared to HiRLoc-II, since several beacons from the communication range variation phase are discarded (see step 2). In addition, the intersection of the ROI with the previous estimate at each transmission round, adds an extra computational step for HiRLoc-II. On the other hand, in HiRLoc-II, the sensor has an estimate of its location at any given time, and does not have to wait for several transmission rounds to compute the ROI. Furthermore, the sensor may choose to terminate the algorithm at some intermediate round, if its location is computed with sufficient accuracy and hence, reducing the computational complexity. Note that in HiRLoc-I, sensors may also compute a ROI estimate at any transmission round if they choose to.

C. Security features of HiRLoc

In order to provide high-resolution robust localization in an untrusted environment, HiRLoc is enforced with the following security features.

Encryption of the beacon transmissions: All the beacons transmitted from locators are encrypted with a globally shared symmetric key K_0, pre-loaded in every sensor and locator before deployment. In addition, every sensor s shares a symmetric pairwise key $K_s^{L_i}$ with every locator L_i, also pre-loaded. In order to reduce the storage requirement at each locator the pairwise keys $K_s^{L_i}$ are derived by a master key K_{L_i}, using a pseudo-random function h [32], and the unique sensor ID_s: $K_s^{L_i} = h_{K_{L_i}}(ID_s)$.

Authentication of the beacon transmissions: In order to prevent holders of the common key K_0 from broadcasting bogus beacons, we provide a mechanism that allows sensors to authenticate the source of the beacons using *collision-resistant hash functions* [32]. Each locator L_i has a unique password PW_i, blinded with the use of a *collision-resistant* hash function h such as SHA1 [32]. By recursive application of the hash function, each locator generates a chain of hash values: $h^0 = PW_i, \quad h^i = h(h^{i-1}), \quad i = 1, \cdots, n,$ with

h^0 never revealed to any sensor. The number n of hash values stored at each locator determines the number of beacon transmissions that each locator can perform and hence, has to be large. Due to the collision resistance property, it is computationally infeasible for any attacker to find a PW_j, such that $h(PW_i) = h(PW_j),\ PW_i \neq PW_j$.

To enable sensors to authenticate a beacon transmission, each sensor is pre-loaded with a table containing the ID_{L_i} of each locator and the corresponding hash value $h^n(PW_i)$. To reduce the locator storage requirements, locators employ an efficient storage/computation method for hash chains of time/storage complexity $\mathcal{O}(\log^2(n))$ [7].

Authentication mechanism: A locator transmitting its j^{th} beacon appends the next hash value $h^{n-j}(PW_i)$ towards the beginning of the hash chain $h(PW_i)$, along with the index j. Every sensor that hears the beacon, hashes the received hash value to verify that $h(h^{n-j}(PW_i)) = h^{n-j+1}(PW_i)$. If the verification is correct, the sensor accepts the beacon information, replaces $h^{n-j+1}(PW_i)$ with $h^{n-j}(PW_i)$ in its memory, and increases the hash counter by one. The hash counter facilitates the synchronization with the latest published hash value, in case of loss of some intermediate hash values. The j^{th} beacon format of locator L_i is as follows:

$$L_i :\ \{\ loc_i \ || \ (h^{n-j}(PW_i)) \parallel j \parallel ID_{L_i}\ \}_{K_0},$$

where $loc_i = (X_i, Y_i) \ || \ (\theta_{i,1}(j), \theta_{i,2}(j)) \ || \ R_i(j)$, $||$ denotes the concatenation operation and $\{m\}_K$ denotes the encryption of message m with key K. Note that our authentication mechanism does not prevent a sensor from authenticating a bogus beacon, if the beacon originates from a locator that is not within the communication range of the sensor. However, our method guarantees that beacons originating from the set of locators directly heard by a sensor s, are indeed authentic. In our threat analysis we will show that this is a sufficient condition for the robust location computation when sensors are under attack.

IV. Security threats against HiRLoc

In this section, we explore the security threats against HiRLoc, that can occur when sensors are deployed in an untrusted environment. We show that HiRLoc allows sensors to perform robust high-resolution location computation even in the presence of malicious adversaries.

A. Attacker model

We assume that the goal of the attacker, is to displace the sensor, i.e. lead the sensor to a location estimation significantly different than its actual location. Furthermore, we assume that the adversary attacking the localization scheme wants to remain undetected by the sensors, or the locators. Hence, we do not consider all possible denial-of-service attacks (DoS) attacks that will prevent the sensor from any location computation. *Note that our defense mechanisms are developed to allow the robust location computation even in the presence of malicious adversaries, and not to prevent the attacks from interrupting other network protocols.*

B. The Wormhole Attack

Threat model: In the wormhole attack discussed in [12], [28], an adversary deploys a direct link referred as *wormhole link* between two points on the network with a distance longer than the communication range. The adversary records any broadcasted information at one end of the wormhole link, known as the *origin point*, tunnels it to the other end of the link, known as *destination point*, and replays the information into the network. Hence, the wormhole attack can be launched without compromising any host, or the integrity and authenticity of the communication and is difficult to detect [12].

Wormhole attack against HiRLoc—antenna orientation variation: An adversary launching a wormhole attack against HiRLoc, records beacons at the origin point, and replays them at the destination point, in order to provide false localization information. Note that since in step 1 of HiRLoc, the sensor determines the set of locators LH_s that are within range, and accepts future transmissions only from that set of locators, the attacker has to replay the recorded beacons in a timely manner, i.e. before the second round of beacon transmissions occurs.

Furthermore, the attacker must continue to forward all subsequent beacon transmissions occurring at the origin point due to the antenna orientation variation, in order to compromise the majority vote scheme used in step 3, and displace the sensor. For example if each locator performs $(Q-1)$ antenna rotations, due to majority voting the attacker has to replay more than $Q|LH_s|$ beacons corresponding to sectors that lead to a ROI different than the sensor's location.

In figure 4(a), the attacker records beacons from two origin points, tunnels them via the wormhole link and replays them to sensor s. Assuming that the attacker replays the beacons in a timely manner, the sensor register as set of locators heard, $LH_s = \{L_1 \sim L_{13}\}$. If all beacons updates are forwarded to the sensor, $4Q$ sectors will intersect around the actual location of the sensor, $4Q$ sectors will intersect around origin point B, and $5Q$ beacons will intersect around the origin point A. Hence, due to the majority vote scheme employed in step three of HiRLoc, the sensor will be displaced in the area of the origin point A. Note that replay from multiple origin points does not increase the effectiveness of the wormhole attack in corrupting the location estimation of a sensor, since the sectors corresponding to different origin points do not overlap.

Defending against the wormhole attack—antenna orientation variation All beacons considered in the ROI computation originate from locators $L_i \in LH_s$ determined in step 1 of HiRLoc. To avoid sensor displacement the sensor must be capable of identifying the valid set of locators LH_s^v from the replayed one, LH_s^r. Since the set LH_s is defined before any antenna rotation, this step is identical to the LH_s determination in SeRLoc [18]. Hence, the mechanisms developed for SeRLoc for identifying LH_s^v can also be employed in the case of HiRLoc. In particular the wormhole attack can be detected due to the following two properties [18]:

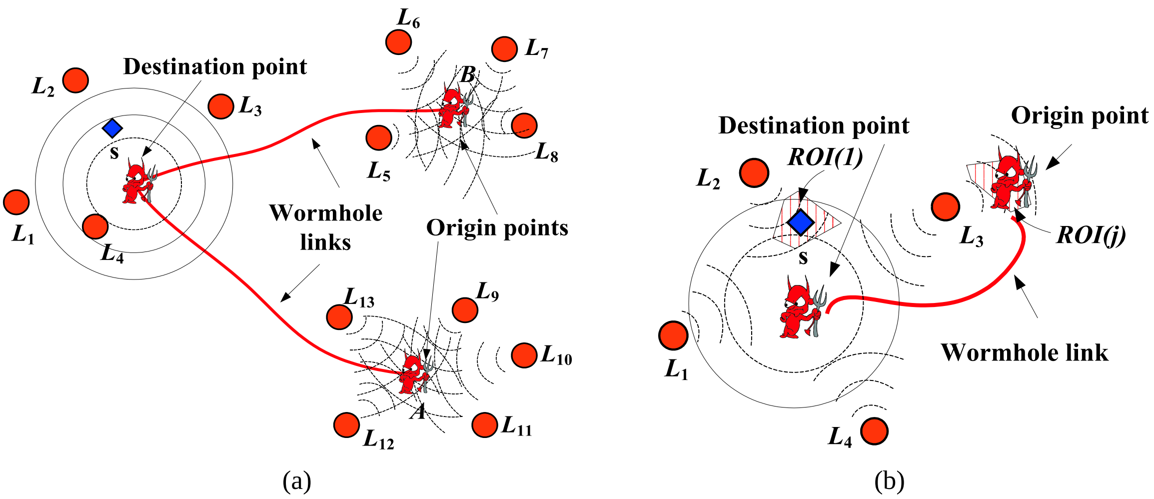


Fig. 4. (a) Wormhole attack—antenna orientation variation: an attacker records beacons in area B, tunnels them via the wormhole link in area A and re-broadcasts them. (b) Wormhole attack—communication range variation: the attacker records and replays beacons from $L_i \in LH_s$ that are not heard at the sensor s when reducing their communication range.

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

2. Communication range violation property: A sensor s cannot hear two locators $L_i, L_j \in LH_s$, more than $2R_{max}$ apart, i.e. $\|L_i - L_j\| \leq 2R_{max},\ \forall L_i, L_j \in LH_s$.

The proofs of properties 1, 2 are provided in [18]. Due to property 1, an adversary cannot replay beacons originating from locators directly heard to the sensor s, since the replays will use an already published hash value. For example, in figure 4(a), if an adversary replays a beacon originating from any antenna of locator L_3,[4] the sensor will already have received a beacon authenticated with an identical hash value from the direct link. Hence, the sensor can detect that is under attack if any such replay occurs. Note that a replay due to multipath effects or imperfect sectorization results in false positives, and will be dropped from the location estimation computations.

Due to property 2, an adversary cannot replay a beacon originating from a locator that is more than $2R_{max}$ apart from any of the set of locators heard to the sensor s under attack. As an example, in figure 4(a), if the adversary replays a beacon from a locator that is more than $2R_{max}$ away from any of the locators $L_1 \sim L_4$, the attack will be detected.

Based on properties 1, 2, it was shown that independent of the location of the origin point(s), any wormhole attack will be detected with a probability very close to unity [18]. In fact, we were able to analytically evaluate the probability of wormhole detection based on the distribution parameters and the communication range of the locator R to be equal to [19]:

$$P_{det} \geq (1 - e^{-\rho_L A_c}) + (1 - e^{-\rho_L A^*})^2 e^{-\rho_L A_c}, \qquad (11)$$

[4]The locators use the same hash value to authenticate all beacons transmitted at different antennas during the same transmission round, and the transmissions occur simultaneously.

$$A^* = x\sqrt{R^2 - x^2} - R^2 \tan^{-1}\left(\frac{x\sqrt{R^2 - x^2}}{x^2 - R^2}\right), \qquad (12)$$

$$x = \frac{l}{2}, \quad A_c = 2R^2\phi - Rl\sin\phi, \quad \phi = \cos^{-1}\frac{l}{2R}. \qquad (13)$$

with l being the distance between the sensor and the origin point of the attack [18]. Once the attack is detected, the sensor can identify the valid set of locators LH_s^v, using the *Attach-to-Closer-Locator* (ACLA) method presented in [18], and use only the beacons originating from the valid set to compute the ROI. In ACLA, a sensor s under attack waits for a small random time before broadcasting a nonce along with its sensor Id, and then awaits for the first authentic reply containing the nonce. Locators that hear the sensor's broadcast reply with the nonce, their ID_{L_i} and localization information, encrypted with the pairwise key $K_s^{L_i}$. Since the closest locator always replies first and is always directly heard to the sensor under attack, the sensor is able to identify the valid set of locators LH_s^v as all the locators less than $2R_{max}$ away from the closest locator and use the corresponding beacons to compute a correct ROI estimate. Note that ACLA, requires that the closest locator has not been compromised. We will investigate the locator compromise in Section IV.D.

Wormhole attack against HiRLoc—communication range variation: When HiRLoc is applied with the communication range variation option (Option B), identifying the set of valid locators from the replayed ones is not sufficient to prevent wormhole attacks. As an example consider figure 4(b), and assume that all locators $L_1 \sim L_4$ are heard to sensor s when they transmit with the maximum transmission power. During step 1 of HiRLoc, the sensor identifies $LH_s = \{L_1 \sim L_4\}$. Assume also that each locator performs N beacon transmissions with different communication ranges, and that only K transmissions are heard at the sensor. An

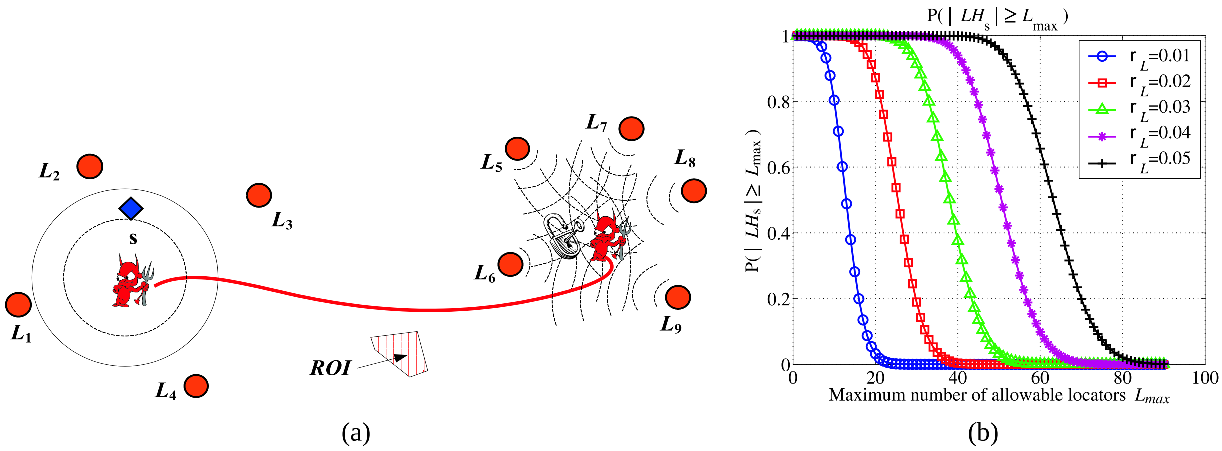


Fig. 5. An adversary assumes the IDs of locators $L_5 \sim L_9$ fabricates bogus beacons and displaces the sensor to an arbitrary location, (b) $P(|LH_s| \geq L_{max})$, vs. L_{max} for varying locator densities ρ_L.

adversary being located at the origin point can record and replay to the sensor up to $(4N - K)$ beacons not heard to the sensor and displace it.

Defending against the wormhole attack—communication range variation In the case of the communication range variation the detection method based on properties 1, 2 cannot prevent the attack as illustrated by the previous example. However, we can still detect a wormhole attack using the following approach:

Instead of computing the ROI after the collection of all beacon transmissions, the sensor computes an estimate of the $ROI(1)$ by using all the beacons transmitted with the maximum communication range. The computation of the $ROI(1)$ is identical to the computation of the ROI in the case of the SeRLoc [18]. Once the initial estimate of the $ROI(1)$ is computed robustly, any subsequent estimation of the $ROI(j)$ must intersect with the initial one. Since subsequent ROI estimates are refinements of $ROI(1)$, if the sensor computes a $ROI(j)$ that does not intersect with the initial one, it detects that it is under attack. Hence, an adversary can only hope to displace the sensor within the region of the initial estimation of the $ROI(1)$.

In our example in 4(b), the sensor initially computes the $ROI(1)$ located around its actual location. The replay of the beacons from the origin point generate a $ROI(j)$ around the origin point that does not intersect with the initial estimate of the $ROI(1)$. Hence, the attack is detected and the beacons intersection in $ROI(j)$ are rejected.

C. Sybil Attack

Threat model: In the Sybil attack [9], [13], [33], an adversary impersonates multiple network entities, by assuming their IDs. In a network where data are encrypted and the ID of each transmitting entity is authenticated, unlike the wormhole attack, the adversary has to both compromise the encryption and authenticity of the communication in order to successfully launch a Sybil attack. In HiRLoc, sensors determine their location based on information transmitted only by locators. Hence, an attacker can only impact the localization if it impersonates locators. In our attack analysis against HiRLoc we focus on locator impersonation.

Sybil attack against HiRLoc—antenna orientation variation: In order for an attacker to impersonate a locator and provide bogus beacon information to a sensor s, the attacker has to, (a) compromise the globally shared key K_0 used for the beacon encryption, (b) acquire a published hash value from a locator not directly heard by the sensor s[5].

Once the attacker compromises K_0, it can record a beacon from a locator not heard by s, decrypt the beacon using K_0, alter the beacon content, and forward the bogus beacon to sensor s. Since the sensor does not directly hear the transmission from the impersonated locator, it will authenticate the bogus beacon. By impersonating sufficient number of locators, the attacker can forward to a sensor s a higher number of bogus beacons than the valid ones, compromise the majority vote scheme, and displace s. In figure 5(a) the attacker decrypts all beacons received from locators $L_5 \sim L_9$ and acquires the published hash values, during all transmission rounds of the antenna orientation variation. Using the hash values it can fabricate any desired beacon and forward it to sensor s. Since the fabricated beacons are more than the valid ones, the sensor is displaced at an arbitrary area.

Defense against the Sybil attack: Since the locators are randomly distributed, on average, each sensor will hear the same number of locators. Hence, when a sensor is under attack, it will hear an unusually high number of locators (more than double the valid ones). We can use our knowledge of the locator distribution to detect the Sybil attack by selecting 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 is under attack and executes ALCA to determine its position. Since ACLA utilizes the pairwise keys $K_s^{L_i}$ to identify the valid set of locators, the Sybil attack will not be successful, unless the attacker compromises locators. We will analyze the locator compromise case in the

[5]The sensor always has the latest published hash values of the hash chains from the locators directly heard by it.

Enhanced Location Resolution Algorithm (ELRA)

s : **broadcast** $\{\ \eta_s \parallel LH_s(1) \parallel ID_s\ \}$
$RL_s = \{L_i : \|s - L_i\| \leq r_{sL}\}$
RL_s : **broadcast** $\{\ \eta_s \parallel LH_s(1) \parallel ID_s \parallel (X_i, Y_i) \parallel H^{n-k}(PW_i) \parallel j \parallel ID_{L_i}\ \}_{K_0}$
$BL_s = \{L_i : \|RL_s - L_i\| \leq r_{LL}\} \bigcap LH_s(1)$
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** *HiRLoc with collected beacons*

Fig. 6. The pseudo-code for the Enhanced Location Resolution Algorithm (ELRA).

next section. The probability that a sensor s hears more than L_{max} locators is:

$$\begin{aligned} P(|LH_s| \geq L_{max}) &= 1 - P(|LH_s| < L_{max} \\ &= 1 - \sum_{i=0}^{L_{max}-1} \frac{(\rho_L \pi R^2)^i}{i!}\ e^{-\rho_L \pi R^2}. \end{aligned} \quad (14)$$

Using (15), 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. In figure 5(b), we show $P(|LH_s| \geq L_{max})$ vs. L_{max}, for varying locator densities ρ_L. Based on figure 5(b), we can select the appropriate value L_{max} for each value of ρ_L.

Sybil attack against HiRLoc—communication range variation: When HiRLoc uses the communication range variation option, an adversary launching a Sybil attack can also impersonate locators $L_i \in LH_s$ when their communication range is reduced so that they are no longer heard to the sensor. For example in figure 5(a), when locator L_4 reduces its communication range and is no longer heard by s, it can be impersonated in a similar way as locators $L_5 \sim L_9$.

In such a case, limiting the number of locators heard to a maximum allowable number does not guarantee that the valid beacons will be more than the fabricated ones. In order to avoid sensor displacement we follow the same approach as in the case of the wormhole attack in the communication range variation option. The sensor computes an estimate of the ROI by using only the beacons with the maximum communication range and by limiting the number of locators heard. Once the initial estimate of the ROI is computed, any subsequent estimation $ROI(j)$ has to intersect with the initial one. Otherwise the sensor detects that is under attack and rejects that estimate. Hence, an adversary can only hope to displace the sensor within the region of the initial estimation $ROI(1)$.

D. Compromised network entities

Network entities are assumed to be compromised when the attacker gains full control over their behavior. While an attacker has no incentive to compromise sensors, since sensors do not actively participate in the localization procedure, compromise of a single locator can potentially lead to the displacement of any sensor in the network [18].

An adversary compromising a locator gains access to both the globally shared key K_0, the master key K_{L_i} used for the construction of all the pairwise keys, as well as the locator's hash chain. During the execution of ACLA, a compromised locator can displace a sensor if it transmits from a location that is closer to the sensor than the closest valid locator. To avoid sensor displacement by a single locator compromise, we strengthen the robustness of the ACLA algorithm by adopting the *Enhanced Location Resolution Algorithm* (ELRA) initially proposed in [19], in order to resolve any location ambiguity. The advantage of ELRA is that it involves replies from more than one locators, so that a single locator compromise is not sufficient to displace a sensor. A sensor s under attack executes the following steps to determine its location.

- *Step 1:* Sensor s broadcasts a nonce η_s, the set of locators heard $LH_s(1)$ in the first transmission round and its ID_s.

$$s:\ \{\ \eta_s \parallel LH_s(1) \parallel ID_s\ \}. \quad (15)$$

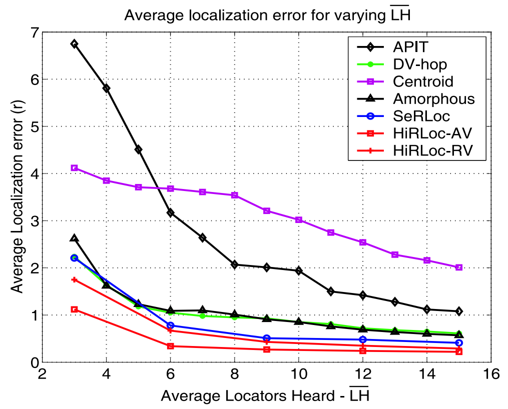
- *Step 2:* Every locator L_i receiving η_s appends its coordinates, the next hash value of its hash chain and its ID_{L_i}, encrypts the message with K_0 and re-broadcasts the message to all sectors with maximum power.

- *Step 3:* Every locator receiving the re-broadcast, verifies the authenticity of the message, and that the transmitting locator is within range. If the verification is correct and the receiving locator belongs to $LH_s(1)$, the locator broadcasts a new beacon with location information and the nonce η_s encrypted with the pairwise key with sensor s.

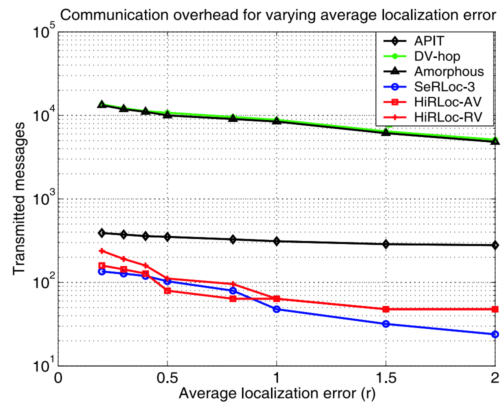
$$L_i:\ \{\ \eta_s \parallel loc_i \parallel H^{n-k}(PW_i) \parallel j \parallel ID_{L_i}\ \}_{K_s^{L_i}}. \quad (16)$$

- *Step 4:* The sensor collects the first L_{max} authentic replies from locators, and selects those L_{max} locators as the valid set. The sensor executes HiRLoc with only the valid set of locators.

The pseudo-code for the ELRA is shown in figure 6. 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



(a)



(b)

Fig. 7. (a) Comparison of the average localization error in units of sensor communication range (r) for varying average number of locators heard at each sensor. SeRLoc, HiRLoc-AV and HiRLoc-RV use three sectored antennas. One locator for SeRLoc and HiRLoc correspond to three locators for all other algorithms. HiRLoc-AV uses only one antenna rotation and HiRLoc-RV uses only one communication range reduction. (b) Comparison of the communication overhead in number of transmitted messages for varying average localization error. HiRLoc-AV uses only one antenna rotation and HiRLoc-RV uses only one communication range reduction.

that the sensor has at least $\frac{L_{max}}{2}$ locators within range R with very high probability (see figure 5(b)), the adversary has to compromise at least $\left(\frac{L_{max}}{2}+1\right)$ locators, in order to displace the sensor under attack.

V. Performance Evaluation

In this section we compare the performance of HiRLoc with state-of-the-art decentralized range-independent localization techniques [3], [10], [18], [25], [26]. We show the improvements achieved when HiRLoc is employing the antenna orientation variation and when HiRLoc is employing the communication range variation method. For our performance evaluation, we randomly distributed 5,000 sensors within a 100x100 m^2 square area and also randomly placed locators within the same area, and for each sensor we computed the ROI for different locator densities ρ_L. We repeated each experiment for 100 networks and averaged the results.

Using the locator density ρ_L we can compute the average number of locators heard by each sensor, as well as the number of locators that need to be deployed in order to cover a specific region with density ρ_L. The average locators heard by each sensor is computed based on (1), and is equal to:

$$\overline{LH} = \rho_L \pi R^2 = \frac{|L|}{\mathcal{A}}\pi R^2, \tag{17}$$

where $|L|$ denotes the total number of locators deployed and $\mathcal{A}$ denotes the size of the deployment region.

For example, if we want each sensor to hear on average 10 locators and the communication range of each locator is equal to $R = 40m$, we need to deploy locators with a density

$$\rho_L = \frac{\overline{LH}}{\pi R^2} = 0.008 \text{ locators}/m^2.$$

Given the locator density, the total number of locators than need to be deployed to cover a $\mathcal{A}$ = 100x100 m^2 square area is equal to $\rho_L\mathcal{A} = 0.008\text{x}10^4 = 80$ locators. Deploying 80 locators is sufficient for each sensor to hear on average 10 locators, independent of the number of sensors deployed within the sensor field. Once the deployment area has been sufficiently covered with locators, an arbitrary number of sensors can be supported within that area.

A. *Localization error vs. Locators heard and Communication overhead*

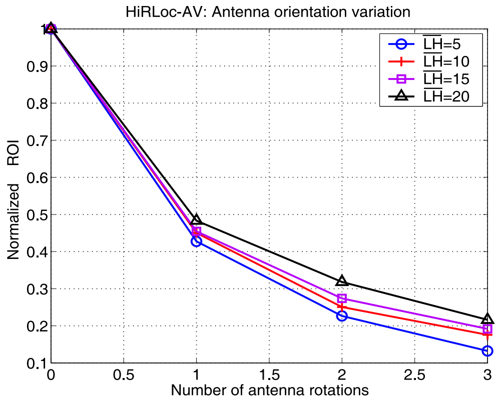
In our first experiment, we examined the impact of the average number of locators heard $\overline{LH}$ on the localization accuracy of HiRLoc and compared it with the state-of-the-art range-independent localization algorithms. We evaluated the average localization error $\overline{LE}$ as:

$$\overline{LE} = \frac{1}{|S|}\sum_{i=1}^{|S|}\frac{\|\hat{s}_i - s_i\|}{r}, \tag{18}$$

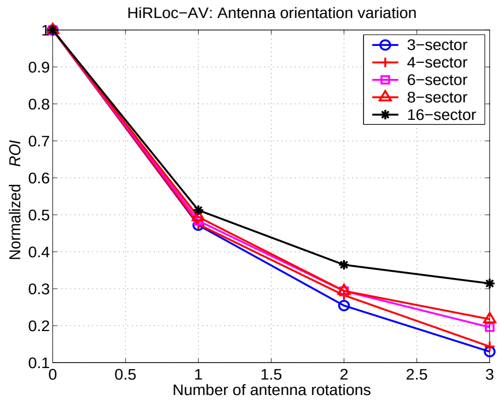
where S denotes the set of sensors deployed within $\mathcal{A}$, $\hat{s}_i$ denotes the location estimate for sensor s_i and s_i denotes the real position of the sensor. For HiRLoc, the location estimate $\hat{s}_i$ of each sensor was computed as the center of gravity of the ROI. In order to provide a fair comparison with methods that do not use directional antennas, we normalized $\overline{LH}$ for HiRLoc by multiplying $\overline{LH}$ with the number of antenna sectors used at each locator.

In figure 7(a) we show the average localization error $\overline{LE}$ in units of sensor communication range r for varying number of locators heard at each sensor. HiRLoc-AV denotes HiRLoc that uses antenna orientation variation to improve upon the accuracy of the location estimate of sensors. HiRLoc-RV denotes HiRLoc that uses communication range variation to improve upon the accuracy of the location estimate of sensors. For HiRLoc-AV and HiRLoc-RV, we performed only one rotation of the antenna at each locator and only one reduction in the communication range, respectively and used 3-sectored antennas.

We can observe that HiRLoc-AV has the best performance among all algorithms while HiRLoc-RV gives the second best performance. The localization error drops rapidly under r even for small values of $\overline{LH}$ while it is equal to $\overline{LE} = 0.23r$ for



(a)



(b)

Fig. 8. (a) Normalized ROI vs. number of antenna rotations for varying $\overline{LH}$. The ROI is normalized with respect to the ROI acquired with no variation of the antenna orientation (application of SeRLoc). (b) Normalized ROI vs. number of antenna rotations for varying size of antenna sectors.

$\overline{LH} = 15$.[6] HiRLoc-AV is superior than HiRLoc-RV for the same value of $\overline{LH}$, since in HiRLoc-AV locators still transmit with the same transmission power once their antenna has been rotated. Hence, the same set of locators is heard at each sensor in any transmission round. On the other hand, in HiRLoc-RV, once the transmission range has been reduced some of the locators heard in the previous round may get out of the range of the sensor and, hence, the improvement in the accuracy of the location estimation using HiRLoc-RV is less than the one achieved with HiRLoc-AV.

In figure 7(b) we show the communication cost required for localization in number of transmitted messages, for varying average localization error $\overline{LE}$. The communication cost was computed for a sensor network of 200 sensors. Note that SeRLoc and HiRLoc are the only algorithms whose communication cost is independent of the number of sensors deployed. All other algorithms rely on neighbor sensor information to estimate the sensor location and, hence, the communication cost grows with the increase of the size of the sensor network.

We observe that for small localization error (less than r) HiRLoc requires less messages for localization compared to all other algorithms. This result seems counter intuitive, since each locators in our experiment had to transmit twice the number of messages compared to SeRLoc. However, fewer locators were required in order to achieve the desired localization accuracy, and, hence, the overall communication cost was lower for HiRLoc. As the required localization accuracy decreases (above r) SeRLoc becomes more efficient than HiRLoc, since it can achieve good precision with a relatively small number of locators. It is important to note that though HiRLoc and SeRLoc have similar performance in communication overhead, HiRLoc needs a much smaller number of locators to achieve the same localization accuracy. This fact becomes evident in the following experiments.

B. Region of intersection—Antenna orientation variation

In our second experiment, we examined the impact of the number of antenna rotations on the size of the ROI. In figure 8(a) we show the ROI vs. the number of antenna rotations, and for varying $\overline{LH}$, when 3-sector antennas are used at each locator. Note that the ROI is normalized over the size of the ROI given by SeRLoc denoted by ROI(1) (no antenna rotation). From figure 8(a), we observe that even a single antenna rotation, reduces the size of the ROI by more than 50%, while three antenna rotations reduce the size to $ROI(4) = 0.12ROI(1)$, when $\overline{LH} = 5$. A reduction of 50% in the size of the ROI by a single antenna rotation means that one can deploy half the locators compared to SeRLoc and achieve the same localization accuracy by just rotating the antenna system at each locator once. The savings in number of locators are significant considering that the reduction in hardware requirements comes at no additional cost in communication overhead.

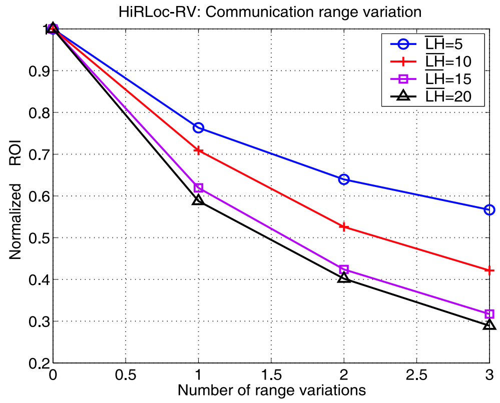
We also observe that as $\overline{LH}$ grows HiRLoc does not reduce the ROI by the same percentage compared to lower $\overline{LH} = 5$. This is due to the fact that when the number of locators heard at each sensor is high, SeRLoc provides an already good estimate of the sensor location (small ROI) and hence, the margin for reduction of the ROI size is limited.

In figure 8(b) we show the normalized ROI vs. the number of antenna rotations, and for varying number of antenna sectors at each locator. As in the case of high $\overline{LH}$, when the antenna sectors become narrow (16-sector antennas) SeRLoc already gives a very good location estimate and hence, HiRLoc does not provide the same improvement as in the case of wider sectors. Furthermore, when the sectors are already very narrow, it would be expensive to develop a mechanism that would rotate the antennas at each locator with great precision. Hence, HiRLoc is very efficient when wide antenna sectors are used at each locator.

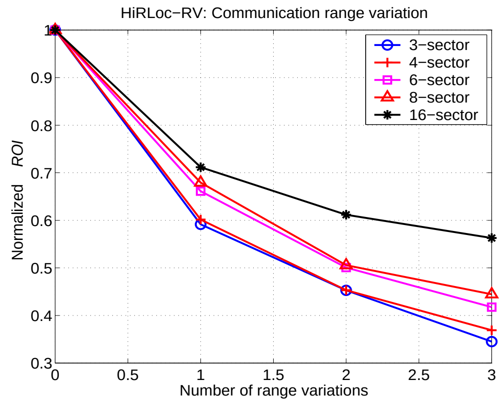
C. Region of Intersection—Communication Range variation

In our third experiment, we examined the impact of the communication range variation on the size of the (ROI). In figure 9(a) we show the normalized ROI vs. the number of communication range variations, and for different $\overline{LH}$ values, when 3-sector antennas are used at each locator. Each locator transmits beacons at four different communication ranges.

[6] $\overline{LH} = 15$ corresponds to each sensor hearing on average 5 locators since locators were equipped with 3-sectored antennas.



(a)



(b)

Fig. 9. (a) ROI vs. number of range reductions for varying $\overline{LH}$. The ROI is normalized with respect to the ROI acquired with no variation of the communication range (application of SeRLoc). (b) Normalized ROI vs. number of range reductions for varying size of antenna sectors.

From figure 9(a), we observe that the communication range variation, though significantly improves the system performance, does not achieve the same ROI reduction as the antenna orientation variation[7]. This behavior is explained by the fact that the gradual reduction of the communication range reduces the number of beacons heard at each sensor, in contrast with the antenna orientation variation case where the same number of locators is heard at the sensors at each antenna rotation. In addition, we observe that greater ROI reduction occurs when the $\overline{LH}$ at each locator is high. This is justified by considering that a higher $\overline{LH}$ allows for more sectors with lower communication range to intersect and hence, smaller ROI.

In figure 9(b), we show the normalized ROI vs. the number of communication range variations, and for varying number of antenna sectors at each locator. Though the ROI reduction is not as high as in the antenna orientation variation case, the communication range variation leads to significant performance improvement. As in our previous experiment, narrower antenna beams give a good location estimate and hence, has smaller margin for improvement.

VI. Related Work

While the problem of localization in a trusted environment has been an extensive topic of research [1], [3], [10], [25]–[27], [30], [31], very few methods have been proposed for secure localization [6], [15], [18]–[22].

Localization schemes proposed for a trusted environment can be classified to 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) [5], [11], time difference of arrival (TDOA) [30], [31], angle of arrival (AOA) [27], or received signal strength indicator (RSSI) [1]. In the range-independent localization schemes, nodes determine their location based only on the information transmitted from the reference points, without using any time, angle, or power measurements [3], [10], [25], [26].

In [18], [19], Lazos and Poovendran propose a range-independent localization scheme called SeRLoc, that uses the properties of the physical medium (communication range constraint) and computationally efficient cryptographic primitives to allows sensors to determine their location, even in the presence of security threats. Sensors rely on localization information transmitted from reference points with known location and orientation, in order to estimate their position. SeRLoc provides secure localization under the assumption that any attacker cannot selectively jam transmissions of reference points. Reference points are equipped with directional antennas in order to provide higher localization accuracy at the sensors. However, further increase of the localization accuracy requires the deployment of more reference points or the use of more directional antennas at each reference point.

In [6] Čapkun and Hubaux propose SPINE, a secure range-based positioning based on bounding the distance of each sensor to at least three reference points. By using timers with nanosecond precision, each sensor can bound its distance to any reference point within range. If the sensor is within a triangle formed by three reference points, it can compute its position via a method called verifiable multilateration. Verifiable multilateration provides a robust position estimate, assuming that any attacker does not collude with compromised nodes. However, in order to perform verifiable multilateration a high number of reference point is required [6].

In [20] Lazos et al. propose ROPE, a range-independent localization scheme that limits the impact of a multiple attacks such as the wormhole attack [12], the Sybil attack [9], [13], [33] and selective jamming, without the need for deploying a large number of reference points. Rope relies on computationally efficient cryptographic primitives to secure the beacon transmissions from the reference points , as well as distance bounding [4], [6] to verify the distance of each sensor to at least one reference point. Hence, any adversary can only displace a sensor within a limited region.

In [22], Liu et al. propose a robust range-dependent local-

[7]The comparison is valid for the same number of $\overline{LH}$, the same number of antenna sectors and the same number of variations in the antenna rotation and communication range, respectively.

ization method that uses Minimum Mean Square Estimation (MMSE) to filter outliers, and compute the position of the sensors using a consistent set of range estimates. The method presented in [22] prevents attackers from displacing sensors by corrupting a small set of range estimates. However, the valid set of range estimates cannot be identified if the attacker successfully corrupts a large set of range estimates (more than the benign ones).

In [21], Li et al. propose the use of robust statistical methods for filtering out the outliers in the sample set used to estimate the sensors' location. The authors illustrate how they can limit the impact of the outliers by employing a Least Median Squares (LMS) technique. As in the case of the method in [22], the authors make the implicit assumption that the majority of the observations collected by each sensor are benign and only a few samples are corrupted. However, in specific types of attacks such as the wormhole [12] and Sybil attack [9], the majority of the samples can be malicious.

VII. Discussion and Open Problems

The localization schemes that have been proposed for robust estimation of the position of sensors in the presence of adversaries can be classified into two main classes. The schemes proposed in [21], [22], do not consider a specific adversarial model. Instead, they consider that some fraction of the localization information is corrupted, while the majority of the observations are benign. The information can be corrupted either due to network faults or due to some type of attack. Using statistical methods, schemes of the first class filter out outliers and estimate the position of sensors by considering only a consistent subset of the set of the collected observations. The schemes proposed in [6], [18]–[20], consider specific adversarial models and examine the potential attacks an adversary can launch in order to disrupt the localization process. Using the characteristics of the adversarial models, schemes of this class propose mechanisms to secure the localization against the different types of feasible attacks.

HiRLoc belongs to the second class of algorithms where a specific adversarial model is considered. We have shown that an adversary cannot disrupt HiRLoc by corrupting range estimates, since no such estimates are used to compute the position of sensors. An attacker can potentially enlarge the communication range of the locators in an effort to displace the sensors. However such an enlargement is equivalent to the wormhole attack that is detected and prevented with a very high probability when using HiRLoc as presented in Section IV-B. An attacker can also attempt to reduce the communication range of the locators. A reduction in communication range does not lead to sensor displacement since any sensor hearing a locator will still be within the nominal communication range even if it has been reduced by some attack.

In addition, an adversary attempting to disrupt HiRLoc gains no benefit from compromising sensor nodes since sensors do not assist in the localization of other sensors. The only usable information extracted from compromising a sensor is the globally shared key K_0. Though a single sensor compromise reveals the K_0, broadcasting with a commonly shared key is the most bandwidth and energy-efficient solution. The adversary can only use K_0 to launch a Sybil attack. However, the Sybil attack can be prevented with a high probability as presented in Section IV-C. In the case where a higher level of security is required compared to the one offered by the globally shared key, one can adopt the broadcast authentication techniques as in [23], [29]. However, both those techniques require time synchronization among all nodes of the network not currently required for HiRLoc.

In HiRLoc, an attacker can successfully displace sensors by compromising a threshold number of locators (reference point). However, as with any localization algorithm, if the coordinate system used to localize the sensor is false, then the location estimation is false. In addition, an adversary is able to displace sensors if it can selectively jam transmissions of locators. HiRLoc is not jamming resistant. However, such a feature can be added in HiRLoc by employing the distance bounding technique presented in [4], [6], [20]. Jamming resistance comes at the expense of hardware complexity, since sensors need to be equipped with clocks of nanosecond precision in order to perform distance bounding.

On the other hand the methods using robust statistical methods [21], [22] do not attempt to prevent any specific type of attack. They provide a robust estimate of the position of the sensors as long as the majority of the observations are benign. Though most observations collected in the whole network may be benign, an adversary can launch attacks to pockets of the network and corrupt the majority of the observations in a confined network region. As an example consider the wormhole attack described in Section IV-B. In such an attack, the beacons replayed by the attacker provide false localization information to a specific set of sensors. For the sensors under attack the localization process is compromised if the replayed beacons are more than the benign ones. Statistical methods that rely on the detection of consistent subsets of information, will fail to discern the replayed beacons from the valid ones and accept the replayed set of beacons as the most consistent one.

Both classes of solutions to the robust sensor localization problem are by no means perfectly secure to adversaries. In fact, due to the resource constraint nature of the sensor devices, there is a tradeoff between the robustness in the location estimation and the hardware and computational complexity. From the related work, it is evident that no single approach can prevent all types of attacks. A multi-modal approach that takes into account multiple features of the sensor network is required in order to build a robust localization system. Finally, a formal classification of the threat models and their direct relation with the localization error is needed.

VIII. Conclusion

We studied the problem of sensor localization in the presence of malicious adversaries and proposed a high-resolution range-independent localization scheme called HiRLoc. We showed that HiRLoc localizes sensors with significantly higher accuracy than previously proposed methods, while requiring fewer hardware resources. Furthermore, we showed that

HiRLoc allows the robust location computation even in the presence of security threats in WSN, such as the wormhole attack, the Sybil attack and compromise of network entities. Our simulation studies confirmed that variation of the transmission parameters at the reference points leads to high-resolution location estimation.

ACKNOWLEDGEMENTS

This work was supported in part by the following grants: Collaborative Technology Alliance (CTA) from ARL, DAAD19-01-2-0011; ONR award, N00014-04-1-0479; ARO grant, W911NF-05-1-0491. We would like to thank anonymous reviewers for their valuable comments.

REFERENCES

[1] P. Bahl and V. Padmanabhan, RADAR: An In-Building RF-Based User Location and Tracking System, In *Proceedings of the IEEE INFOCOM,* Tel-Aviv, Israel, March 2000, pp. 775–784.

[2] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. Woodward, A Distance Routing Effect Algorithm for Mobility (DREAM), In *Proceedings of MOBICOM,* Dallas, TX, USA, Oct. 1998, pp.76–84

[3] N. Bulusu, J. Heidemann and D. Estrin, GPS-less Low Cost Outdoor Localization for Very Small Devices, In *IEEE Personal Communications Magazine,* 7(5):28-34, Oct. 2000.

[4] S. Brands and D. Chaum, Distance-bounding protocols, In Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 344-359. Springer-Verlag New York, Inc., 1994.

[5] S. Čapkun, M. Hamdi and J. Hubaux, GPS-Free Positioning in Mobile Ad-Hoc Networks, In *Proceedings of HICCSS,* Maui, Hawaii, USA, Jan. 2001, pp. 3481–3490.

[6] S. Čapkun, J. Hubaux, Secure Positioning of Wireless Devices with Application to Sensor Networks, In *Proceedings of the IEEE INFOCOM,* 2005.

[7] D. Coppersmith and M. Jakobsson, Almost optimal hash sequence traversal, In *Proceedings of the FC,* Lecture Notes in Computer Science, IFCA, Springer-Verlag, Berlin Germany, 2002, pp. 102–119.

[8] N. Cressie, *Statistics for Spatial Data,* John Wiley & Sons, 1993.

[9] J. Douceur, The Sybil Attack, In *Proceedings of IPTPS 2002,* Lecture Notes in Computer Science, Vol. 2429 Cambridge, MA, USA, March 2002, pp. 251–260.

[10] T. He, C. Huang, B. Blum, J. Stankovic and T. Abdelzaher, Range-Free Localization Schemes in Large Scale Sensor Network, In *Proceedings of MOBICOM,* San Diego, CA, USA, Sept. 2003, pp. 81–95.

[11] B. Hofmann-Wellenhof, H. Lichtenegger and J. Collins, *Global Positioning System: Theory and Practice,* Fourth Edition, Springer-Verlag, 1997.

[12] Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks, In *Proceedings of INFOCOM,* San Francisco, CA, USA, April 2003, pp. 1976-1986.

[13] J. Newsome, E. Shi, D. Song and A. Perrig, The Sybil Attack in Sensor Networks: Analysis and Defenses, In *Proceedings of the Third International Conference on Information Processing in Sensor Networks,* IPSN 2004, pp. 259–268.

[14] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, In *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications,* May 2002.

[15] M. G. Kuhn, An Asymmetric Security Mechanism for Navigation Signals, In *Proceedings of the Information Hiding Workshop*, 2004.

[16] L. Lamport, Password Authentication with Insecure Communication, In *Communications of the ACM,* 24(11):770 − 772, November 1981.

[17] L. Lazos and R. Poovendran, Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information, In *Proceedings of IEEE ICASSP,* Hong Kong, China, April 2003, Vol. 6, pp. 201–204.

[18] L. Lazos and R. Poovendran, SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks, to appear in *Proceedings of WISE,* Philadelphia, PA, Oct. 2004, pp. 21–30.

[19] L. Lazos and R. Poovendran, Robust Range-independent Localization for Wireless Sensor Networks, to appear In *Transactions on Sensor Networks,* available upon request.

[20] L. Lazos, S. Capkun, and R. Poovendran, ROPE: Robust Position Estimation in Wireless Sensor Networks, In *Proceedings of the Fourth International Conference on Information Processing in Sensor Networks*, IPSN 2005, pp. 324–331.

[21] Z. Li, W. Trappe, Y. Zhang, and B. Nath, Robust Statistical Methods for Securing Wireless Localization in Sensor Networks, In *Proceedings of Proceedings of the Fourth International Conference on Information Processing in Sensor Networks*, IPSN 2005, pp. 91–98.

[22] D. Liu, P. Ning, and W. Du, Attack-Resistant Location Estimation in Sensor Networks, In *Proceedings of Proceedings of the Fourth International Conference on Information Processing in Sensor Networks*, IPSN 2005, pp. 99–107.

[23] D. Liu, P. Ning, Multi-Level μTESLA: Broadcast Authentication for Distributed Sensor Networks, In *Proceedings of the ACM Transactions in Embedded Computing Systems (TECS),* Vol. 3, No. 4, pages 800–836, Nov 2004.

[24] MICA Wireless Measurement System, available at: http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA.pdf.

[25] R. Nagpal, H. Shrobe, J. Bachrach, Organizing a Global Coordinate System from Local Information on an Ad Hoc Sensor Network, In *Proceedings of IPSN,* Palo Alto, USA, April, 2003, Lecture Notes in Computer Science, Vol. 2634, pp. 333–348.

[26] D. Nicolescu and B. Nath, Ad-Hoc Positioning Systems (APS), In *Proceedings of IEEE GLOBECOM,* San Antonio, TX, USA, Nov. 2001, Vol. 5, pp. 2926–2931.

[27] D. Niculescu and B. Nath, Ad Hoc Positioning System (APS) using AoA, In *Proceedings of INFOCOM,* San Francisco, CA, USA, March 2003, Vol. 3, pp. 1734–1743.

[28] P. Papadimitratos and Z. J. Haas, Secure Routing for Mobile Ad Hoc Networks, in *Proceedings of CNDS*, Jan. 2002.

[29] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, SPINS: Security protocols for sensor networks, In *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networks,* 2001, pp. 189–199.

[30] N. Priyantha, A. Chakraborthy and H. Balakrishnan, The Cricket Location-Support System, In *Proceedings of MOBICOM,* Boston, MA, USA, Aug. 2000, pp. 32-43.

[31] A. Savvides, C. Han and M. Srivastava, Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors, In *Proceedings of MOBICOM,* Rome, Italy, July 2001, pp. 166-179.

[32] D. Stinson, *Cryptograhpy: Theory and Practice,* 2nd edition, CRC Press, 2002.

[33] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning, Defending Sybil Attacks in Sensor Networks, In *Proceedings of the International Workshop on Security in Distributed Computing Systems* (SDCS-2005), June 2005.

Loukas Lazos is a Ph.D. student in the Electrical Engineering Department at University of Washington in Seattle. He received his M.S. degree from the same department in 2002 and his B.S. degree from the National Technical University of Athens, Greece, in 2000. His current research interests focus on cross-layer designs for energy-efficient key management protocols for wireless ad-hoc networks, as well as secure localization systems for sensor networks.

Radha Poovendran has been an assistant professor at the Electrical Engineering Department of the University of Washington at Seattle since September 2000. He received his Ph.D. in Electrical Engineering from the University of Maryland, College Park in 1999. His research interests are in the areas of applied cryptography for multiuser environment, wireless networking, and applications of Information Theory to security. He is a recipient of the Faculty Early Career Award from the National Science Foundation (2001), Young Investigator Award from the Army Research Office (2002), Young Investigator Award from the Office of Naval Research (2004), and the 2005 Presidential Early Career Award for Scientists and Engineers, for his research contributions in the areas of wired and wireless multiuser security.