ROPE: ROBUST POSITION ESTIMATION IN WIRELESS SENSOR NETWORKS

Loukas Lazos and Radha Poovendran
Network Security Laboratory (NSL)
Department of Electrical Engineering
University of Washington, Seattle, WA, 98195
{l_lazos, radha}@ee.washington.edu

Srdjan Čapkun
Networked & Embedded Systems Laboratory (NESL)
University of California, Los Angeles
Los Angeles, CA, 90095
Email: capkun@ucla.edu

Abstract— We address the problem of secure location determination, known as *Secure Localization*, and the problem of verifying the location claim of a node, known as *Location Verification*, in Wireless Sensor Networks (WSN). We propose a robust positioning system we call ROPE that allows sensors to determine their location without any centralized computation. In addition, ROPE provides a location verification mechanism that verifies the location claims of the sensors before data collection. We show that ROPE bounds the ability of an attacker to spoof sensors' locations, with relatively low density deployment of reference points. We confirm the robustness of ROPE against attacks analytically and via simulations.

I. INTRODUCTION

Knowledge of the position of the sensing nodes in a Wireless Sensor Network (WSN) is an essential part of many sensor network operations and applications. Sensors reporting monitored data need to also report the location where the information is sensed, and hence, sensors need to be aware of their position. In addition, many network protocols such as routing [2] require location information in order to provide the specific protocol service.

Positioning in WSN has been a topic of extensive research, leading to numerous positioning systems that provide an estimation of the sensor location, based on a variety of mechanisms [1], [4], [6], [10], [18], [19], [21]. However, almost all previously proposed localization techniques are designed for a trusted environment, where all network nodes operate in an honest and cooperative manner, and no external attacks are feasible.

WSN may be deployed in hostile environments where malicious adversaries attempt to spoof the locations of the sensors by attacking the localization process. For example, an attacker may alter the distance estimations of a sensor to several reference points, or replay beacons from one part of the network to some distant part of the network, thus providing false localization information. Hence, we need to ensure that the location estimation is performed in a robust way, even in the presence of attacks. Furthermore, adversaries can compromise the untethered sensor devices and force them to report a false location to the data collection points. Therefore, a secure positioning system must have a mechanism to verify the location claim of any sensor.

The current localization methods [1], [4], [6], [10], [18], [19], [21] are vulnerable to most attacks in WSN, since they were *not* designed based on an adversarial model. Both secure localization and location verification are fairly unexplored areas of research. Brands and Chaum [3] have proposed a location verification method based on a distance bounding protocol that verifies that two nodes connected by a wired link of size d, cannot claim to be at a distance closer than d. In [20], Sastry, Shankar and Wagner proposed a location verification protocol that utilizes both RF and ultrasound signals to bound the distance between two nodes. Recently, Kuhn proposed an asymmetric security mechanism for securing navigation signals [12], such as commercial GPS.

To the best of our knowledge only two methods have been proposed for secure localization in WSN. In [7], Čapkun and Hubeaux proposed SPINE, a secure positioning system based on distance bounding and verifiable multilateration. SPINE is a range-dependent secure positioning scheme, that estimates the location of a sensor by verifying the distances of the sensor to at least three reference points. The location estimation is performed centrally and once a sensor is aware of its location it also becomes a reference point. Hence, sensors rely on other sensors as well as the central authority to securely acquire their location. Though SPINE is robust against attacks in WSN, it requires the deployment of a high number of reference points to achieve localization. In [16], Lazos and Poovendran proposed SeRLoc, a decentralized range-independent localization scheme that achieves secure localization based on beacons transmitted from reference points. In SeRLoc, sensors passively determine their location with no assistance from other sensors, and a relatively small number of reference points is sufficient to localize all sensors. However, SeRLoc is based on the assumption that no jamming of the wireless medium is feasible.

In this paper we present a positioning system called RObust Position Estimation (ROPE) that limits the ability of an adversary to spoof a sensor's location by launching well known attacks in WSN [8], [11]. To quantify the impact of attacks against our positioning system, we introduce a novel metric called Maximum Spoofing Impact (MSI) that denotes the maximum distance between the actual location of the sensor under attack, and any possible spoofed location. Compared to SeRLoc [16], ROPE is resistant to jamming of the communication medium, limits the MSI and prevents location spoofing due to the Sybil attack, unless a significant number of reference points have been compromised. Compared to SPINE [7], ROPE requires the deployment of a significantly smaller number of reference points.

Furthermore, ROPE is a sensor initiated localization procedure, that allows sensor to request an update of their position, whenever it becomes outdated. Finally, we provide quantitative arguments to show that ROPE is scalable in storage and communication with the WSN size envisioned in the future, despite the use of pairwise communication to secure the position estimation.

The remainder of the paper is organized as follows: In Section II, we state our problem, present necessary background and related work. In Section III, we state our network model and describe ROPE. In Section IV, we present the security analysis on ROPE. In Section V, we evaluate the resilience of ROPE in security threats via simulation and in Section VI, we present our conclusions.

II. Problem statement & Background

A. Problem statement

We address the problem of robust computation of the location of sensors in WSN, in the presence of malicious adversaries. We will refer to this problem as *Secure Localization*. Note that our goal is only to secure the localization process and hence, we are not concerned with attacks against any other network protocol. Furthermore, our goal is to ensure that an attacker cannot force a sensor to falsely estimate its location while it remains undetected.

We also address the problem of verifying the location claim of a sensor, referred as *Location Verification*. Since every sensor reports its monitoring information to the data collection points within its range, in our location verification we only verify that an out-of-range sensor cannot appear to be in-range. Making an in-range sensor appear out-of-range is of no use to the attacker and hence, it is not addressed.

B. Background

Distance Bounding: Distance bounding protocols are used to verify that a claimant node u being at a distance d_{uv} from a verifier node v, cannot claim to be at a distance $d'_{uv} < d_{uv}$. These protocols were first introduced by Brands and Chaum [3] to prevent Mafia Fraud attacks. As shown in [7], in order for distance bounding protocols to resist distance reduction attacks the distance measurement must be performed with the exchange of RF signals. Any use of a slower medium such as ultrasound, allows to a claimant u to appear closer to the verifier v than it actually is.

The pseudocode for the distance bounding protocol is shown in Figure 1. Initially, the claimant u commits to a random nonce N_u. The verifier replies to u with a challenge nonce N_v, which is sent in the reverse order, and starts its timer as soon as the last bit of the challenge has been sent. The claimant u responds to v with $N_v \oplus N_u$, immediately upon receiving the challenge from v. Once the verifier has received $N_v \oplus N_u$, it stops the timer and converts the challenge-response time t_{vu} to a distance d_{vu}. In the last step of the protocol, u authenticates itself to v by revealing the decommit value $\hat{d}$ via a transmission encrypted with the pairwise key K_{vu}. Finally, v verifies if the value N_u received in the time-measuring phase corresponds to the received commit, decommit pair $(c, \hat{d})$.

The commitment made by the claimant must satisfy two properties: (i) the party who commits to a certain value N_u cannot change N_u after the commitment is made (we say that the scheme is *binding*), (ii) the commitment is hidden from the receiver until the sender "opens" it (we say that the scheme is *hiding*). A commitment scheme is both binding and hiding if it transforms a value m into a commitment/opening pair (c, d), where c reveals no information about m, but (c, d) together reveal m, and it is infeasible to find $\hat{d}$ such that $(c, \hat{d})$ reveals $\hat{m} \neq m$. Efficient commitment schemes can be realized with collision-resistant hash functions such as SHA1 [22], which do not impose high computational requirements on sensors.

In order for the distance bounding protocol to be accurate the claimant u must be able to bound its processing (XOR) to a few nanoseconds, and the verifier v needs to be able to measure time with nanosecond precision ($1ns$ corresponds to the time that it takes an electromagnetic wave to propagate over 30 cm). Current technology allows nanosecond processing and time measurements only with dedicated hardware. RF time of flight systems based on Ultra Wide Band (UWB) can achieve nanosecond precision of measured times of signal flight (and consequently of the distances), thus providing two- and three-dimensional location of objects to within a few centimeters [9]. The range of the system in [9] is 100m indoor

u :	**Generate** random nonce N_u
:	**Generate** commitment $(c, d) = \text{commit}(N_u)$
$u \rightarrow v$:	c
v :	**Generate** random nonce N_v
$v \rightarrow u$:	N_v *(bits sent from MSB to LSB)*
$u \rightarrow v$:	$\hat{N}_u \oplus N_v$ *(bits sent from LSB to MSB)*
v :	**Measure** time t_{vu} between sending N_v and receiving $N_u \oplus N_v$
$u \rightarrow v$:	$E_{K_{vu}}(u, N_u, N_v, d)$
v :	**Decrypt** message and verify if $\hat{N}_u = \text{open}(c, d)$

Fig. 1. Pseudocode for the distance bounding protocol.

and 2km outdoor, with the devices used being roughly the size of a wristwatch, weighing approximately 40 grams each.

Verifiable multilateration: In [7], Čapkun and Hubeaux proposed *Verifiable Multilateration* (VM), a technique that enables secure computation and verification of the positions of wireless nodes in the presence of attackers. In VM at least three reference points (verifiers) v_1, v_2, v_3, independently perform distance bounding to the wireless device (claimant) and communicate the distance bounds db_1, db_2, db_3 to a Central Authority (CA). The CA estimates the claimant's position based on the known position of the verifiers and the distance bounds db_1, db_2, db_3 by the Minimum Mean Square Estimate (MMSE) method or any other method that ensures robust position computation. Subsequently, two tests are run: (i) does the computed position differ from the measured distance bounds db_1, db_2, db_3 by less than the expected distance measurement error δ and (ii) does the computed position fall within the physical triangle $\triangle(v_1, v_2, v_3)$ formed by that triplet of verifiers. If both tests are positive, the CA considers the position of the node to be *valid*; else, the authority considers the position to be *invalid*.

VM relies on the property of distance bounding, that neither the attacker or the claimant can reduce the measured distance of the claimant to the verifier, but only enlarge it. If the node is positioned within the triangle formed by the verifiers and any of the three distance bounds has been enlarged, the attacker would need to reduce one or both of the remaining distance bounds in order to make the enlarged distance bound consistent with the other distance bounds. The same principle applies in three dimensions, where four verifiers form a triangular pyramid. VM prevents attackers from spoofing positions of honest nodes, launching wormhole [11] and jamming attacks, while it prevents dishonest nodes from lying about their positions.

Secure Range-Independent Localization: In [16], Lazos and Poovendran proposed a Secure Range-independent Localization (SeRLoc) scheme based on a two tier network architecture that achieves decentralized passive localization. The sensors rely on beacons transmitted from reference points called *locators*, with known position and orientation, in order to determine their position. Each locator is equipped with directional antennas, thus covering different sector areas with different transmissions. At each sector, the locator transmits its position, and the slopes of the boundaries of the sector where the transmission takes place, referred to a commonly known axis. In Figure 2(a), we show the localization information that is transmitted by a locator L_i, at one of its sectors.

A sensor s hearing a beacon from locator L_i has to be included within the sector area S_i indicated by the localization information embedded in the beacon. The sensor collects beacons from all the locators within range, determines the sector areas S_i where it is
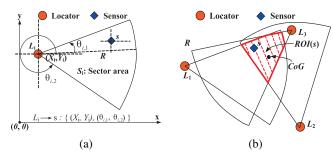
Fig. 2. (a) Each locator L_i transmits at each sector its location (X_i, Y_i), and the slopes of the boundary lines that define the sector area S_i. A sensor s hearing the transmission of L_i is included within the sector S_i. (b) The sensor s defines its position as the CoG of the ROI(s) of all the sectors S_i that include s.

located and estimates its position $\hat{s}$ as the Center of Gravity (CoG) of the Region of intersection (ROI) of all sectors S_i.

$$\hat{s} = CoG(ROI(s)) = CoG \bigcap_{i=1}^{|LH_s|} S_i \quad , \quad (1)$$

where $|LH_s|$ denotes the cardinality of the set of locators heard to sensor s. In Figure 2(b), we show how sensor s determines its position as the CoG of the ROI, computed by the intersection of the S_i heard by locators $L_1 \sim L_5$. Note that sensor localization is achieved passively, without any communication of the sensors with any locators or other sensors.

In SeRLoc, sensors are able to detect attacks against WSN such as the wormhole attack [11] and the Sybil attack [8], with a probability very close to unity assuming that no jamming of the wireless medium has occurred. However, if jamming is feasible the attacker can spoof the location of any sensor.

III. ROPE: Robust Position Estimation

A. Network model assumptions

We assume a two-tier network comprised of sensor devices randomly deployed to sense the environment, and reference points we call *locators*, also randomly deployed to, (a) enable sensors to determine their position by broadcasting localization information, (b) verify the origin of the sensed information, and (c) serve as data collection points.

Sensors: Sensors are randomly deployed in an area $\mathcal{A}$ with a density ρ_s, are equipped with omnidirectional antennas, and have a sensor-to-sensor communication range equal to r. We assume that sensors can bound the processing time for performing simple operations such as XOR to a few nanoseconds, and can measure time with nanosecond precision. Such requirements are essential for performing distance bounding with a satisfactory accuracy and can nowadays be satisfied only using UWB [9].

Locators: Locators are also randomly deployed within the same area $\mathcal{A}$ with a density $\rho_L \ll \rho_s$ (significantly fewer locators are deployed compared to the number of sensors), are equipped with M directional antennas of beamwidth $\frac{2\pi}{M}$ each, and have a locator-to-sensor communication range $R > r$. Due to the antenna directivity gain G of the locators' antennas, the sensor-to-locator communication range r_{sL} is longer than r. If γ denotes the signal attenuation factor, r_{sL} can be computed to be $r_{SL} = rG^{\frac{1}{\gamma}}$ [16]. To give a sense of the required transmission ranges, typical sensors have a communication range of $r = 3 \sim 30m$ [15] with a transmission power of $P_s = 0.75mW$. If locators are required to achieve a ratio of $\frac{R}{r} = 10$, they need to transmit with a power of $P_L = 75mW$, without taking into account the antenna directivity gain and when the attenuation factor

is assumed to be $\gamma = 2$. The directionality of the antennas at the locators reduces the power consumption for achieving the desired $\frac{R}{r}$ ratio.

Furthermore, locators are assumed to have known position and orientation either via manual insertion or a secure GPS system [12]. Note that the assumption of known position and orientation for the locators is essential for any localization algorithm since no absolute location estimate can be obtained without a coordinate system. We further assume that locators can perform nanosecond processing and time measurements, required for distance bounding.

Security assumptions: We assume that both sensors and locators are capable of performing basic cryptographic operations and manage cryptographic primitives. In detail, each sensor s shares a pairwise key $K^s_{L_i}$ with each L_i. To reduce the storage at each locator, pairwise keys are derived from a master key K_{L_i} by the application of a pseudo-random function [22], to the sensor ID. Sensors need not store many pairwise keys, since ROPE requires the deployment of a small number of locators. In the case of a very large network, storage scalability can be ensured by a clustered approach where sensors are pre-loaded only with the pairwise keys associated with the locators covering a specific sub-region of the deployment region.

B. Description of the ROPE algorithm

We now describe our **Ro**bust **P**osition **E**stimation algorithm (ROPE), that provides both the location determination and location verification function.

Location determination: A sensor s determines its location executing the following steps:

Step 1: The sensor broadcasts its Id_s and a random nonce N_s.

$$s : Id_s \parallel N_s.$$

Step 2: Any locator L_i that can communicate bi-directionally with the sensor s performs distance bounding with s. Distance bounding verifies that sensor s is indeed within the vicinity of L_i, and enables the sensor s to define the set LDB_s:

$$LDB_s = \{L_i : \|L_i - s\| \le rG^{\frac{1}{\gamma}}\}. \quad (2)$$

Step 3: If $|LDB_s| \ge 3$ the sensor s checks if it can perform Verifiable Multilateration (VM). VM can only be performed if the sensor lies inside a triangle formed by three locators $L_i \in LDB_s$. If VM is possible, the sensor computes its location, notifies locators $L_i \in LDB_s$ via a transmission encrypted with each pairwise key $K^s_{L_i}$ that the location has been estimated, and terminates the algorithm. Otherwise, for each locator $L_i \in LDB_s$, it computes the disc D_i, according to the distance bound. Then, s computes the Distance Bounding Intersection Region ($DBIR(s)$) as the intersection of all D_i.

$$DBIR(s) = \bigcap_{i=1}^{|LDB_s|} D_i. \quad (3)$$

Step 4: If locators $L_i \in LDB_s$ have not received a termination notification, they re-broadcast the initial sensor message along with their own Id_{L_i}. The re-broadcast is guaranteed to cover all locators heard by sensor s (within a range of R from the sensor) since directional antennas are used both at the receiver and the transmitter. In specific, the re-broadcast covers a range of $RG^{\frac{2}{\gamma}} > R + rG^{\frac{1}{\gamma}}$.
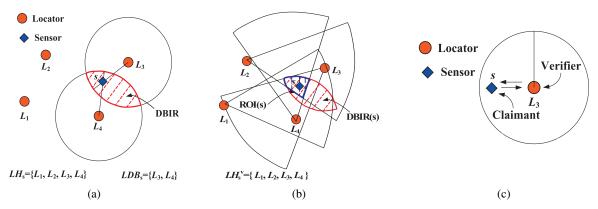
Fig. 3. (a) The sensor s performs distance bounding with locators L_3, L_4 and determines the $DBIR(s)$, (b) the sensor s computes the $ROI(s)$ as the region of $DBIR(s)$ where more sectors of the set LH_s^v intersect. LH_S^v denotes the locators $L_i \in LH_s$ whose sectors intersect with the $DBIR(s)$, (c) sensor s proves its proximity to locator L_3.

Step 5: Locators L_j that hear the broadcast of a locator $L_i \in LDB_s$, transmit at each sector S_j^k the following information:

$$M_j^k, MAC_{K_{L_j}^s}(M_j^k) \quad ,$$
$$M_j^k : Id_{L_j} \parallel (X_j, Y_j) \parallel (\theta_{j,1}^k, \theta_{j,2}^k) \parallel N_s,$$

where M_j^k denotes the message transmitted from the jth locator at the kth sector, $\parallel$ denotes the concatenation operation, Id_{L_j} denotes the locator Id, (X_j, Y_j) denote the coordinates of the locator L_j, $(\theta_{j,1}^k, \theta_{j,2}^k)$ denote the slopes of the boundaries of the kth sector of locator L_j, N_s denotes the nonce initially broadcasted by sensor s, and $MAC_{K_{L_j}^s}(M_j^k)$ denotes the Message Authentication Code for message M_j^k, generated with the pairwise key $K_{L_j}^s$, shared between L_j and s.

The message authentication code is used to preserve the integrity of the message and prove the authenticity of the source. Since only locator L_j has knowledge of the pairwise key $K_{L_j}^s$ besides the sensor s, and it is computationally infeasible for an attacker to find M', K' such that $MAC_{K'}(M') = MAC_{K_{L_j}^s}(M_j^k)$, the sensor upon receipt of any beacon claimed to be from locator L_j can verify that, (a) the message indeed originated from locator L_j and, (b) the message has not been altered in transit.

The nonce N_s broadcasted by the sensor and replayed by the locator is used to provide message freshness. The sensor starts a timer when its initial broadcast occurs and waits for beacon replies only for a limited amount of time. Once the pre-specified time interval has expired, beacons including N_s are rejected.

Step 6: The sensor s collects all valid beacons transmitted from locators within range.

$$LH_s = \{L_i : \|L_i - s\| \leq R\}. \quad (4)$$

Step 7: The sensor defines the set of locators LH_s^v as all locators $L_i \in LH_s$ whose sectors S_i intersect with $DBIR(s)$. Then it defines the Region of Intersection (ROI) as the region of $DBIR(s)$ where

most sectors S_i from locators in the set LH_s^v intersect.

$$LH_s^v = \{L_i \in LH_s : DBIR(s) \bigcap S_i \neq \emptyset\}, \quad (5)$$

$$DS_k = \{L_i \in LH_s^v : \bigcap_{i=1}^{k} S_i \neq \emptyset, 1 \leq k \leq |LH_s^v|\},$$

$$DS = \arg\max_k DS_k, \quad (6)$$

$$ROI(s) = DBIR(s) \bigcap_{i=1}^{|DS|} S_i . \quad (7)$$

Note that in Step 3, if a sensor is included within a triangle of three locators of the set LDB_s it performs VM. VM can be performed by the sensor itself in the absence of a CA, since the sensor is aware of the locators' positions via the beacon transmissions. Hence, ROPE does not require any central computation and the sensor estimates its own position.

In Figure 3(a), the sensor s identifies the set of locators heard $LH_s = \{L_1 \sim L_4\}$, and the set of locators that can perform distance bounding as $LDB_s = \{L_3, L_4\}$. Since $|LDB_s| < 3$, the sensor cannot be included within a triangle of locators and hence, it defines the $DBIR(s)$ as the intersection of the discs D_3, D_4 obtained from the distance bounds from locators D_3, D_4. Observe that the sensor s may be located anywhere within the $DBIR$ since the distance bounds db_3, db_4 may have been enlarged. However the distance bounds cannot be enlarged beyond the sensor-to-locator communication range $r_{sL} = rG^{\frac{1}{\gamma}}$. In Figure 3(b), sensor s defines the set $LH_s^v = \{L_1 \sim L_4\}$ since all sectors S_i intersect with the $DBIR$ and computes the $ROI(s)$ as the intersection of $DBIR(s)$, with all the sectors $S_i, i = 1 \ldots 4$. In Figure 4, we present the pseudocode for ROPE.

Location verification: Locators can also operate as data collection points since every sensor can communicate with at least one locator. In the case a sensor reports data to a locator, the locator needs to verify the sensor's position to ensure that the data being reported corresponds to the region claimed by the sensor.

Though we could provide a high accuracy location verification protocol by involving multiple locators, we adopt a simple scheme where only the locator receiving the data report verifies the distance to the claimant sensor. The locator L_i verifies that a sensor located at a distance db from L_i, cannot claim to be at a distance $db' < db$. Though distance enlargement is possible (the sensor can appear further away from the locator than it actually is), this is of no use to

ROPE: Robust Position Estimation Scheme

s : **broadcast** $Id_s \parallel N_s$
for all L_i *that receive broadcast from* s
    L_i : **perform** *Distance Bounding with* s
    s : **define** $LDB_s = \{L_i : \|L_i - s\| \leq rG^{\frac{1}{\gamma}}, L_i \in LH_s\}$
    if $\exists \{L_i, L_j, L_k\} \in LDB_s$ *such that*
        s *inside* $\triangle L_i L_j L_k$
        s : **compute** $\hat{s}$:=Verifiable Multilateration
        s : **notify** $E_{K^s_{L_i}}(Termination), \forall L_i \in LDB_s$
    else
    L_i : **broadcast** $Id_s \parallel N_s \parallel Id_{L_i}$
endfor
for all L_j *that receive broadcast from* L_i
    L_j : **generate** $M_j^k : Id_{L_j} \parallel (X_j, Y_j) \parallel (\theta_{j,1}, \theta_{j,2}) \parallel N_s, \ k = 1 \dots M$
    L_j : **transmit** $M_j^k, MAC_{K^s_{L_j}}(M_j^k)$, $k = 1 \dots M$
endfor
s : **define** $LH_s = \{L_i : \|s - L_i\| \leq R, \ MAC = valid, \ t_r < T_{expire}\}$
s : **define** $D_i : \|L_i - s\| < db_i, \forall L_i \in LDB_s$
$DBIR(s) = \sum_{i=1}^{|LDB_s|} D_i$
$LH_s^v = \{L_i \in LH_s : DBIR(s) \cap S_i \neq \emptyset\}$
$DS_k = \{L_i \in LH_s^v : \cap_{i=1}^{k} S_i \neq \emptyset, 1 \leq k \leq |LH_s^v|\}$
$DS = \arg\max_k DS_k$
$ROI(s) = DBIR(s) \cap \bigcap_{i=1}^{|DS|} S_i$

Fig. 4. The pseudo-code for the Robust Position Estimation (ROPE) scheme.

---

a dishonest sensor or an attacker, since the sensor will not be able to report its data to a locator outside the communication range r_{sL}. In Figure 3(c), sensor s proves its proximity to locator L_3, by the execution of the distance bounding protocol.

C. Discussion on ROPE

In ROPE, sensors initiate the localization process, by demanding localization information to be transmitted when desired. This feature allows for a mobile sensor network where both locators and sensors may change positions. Since sensors are energy limited devices, they are expected to have limited mobility and hence, not change their position very frequently. In any case, once their position is changed, they can request new localization information from the nearby locators (sensors' position may be outdated while moving) and re-estimate their new position. Sensor initiated localization is a prefered strategy compared to strategies where the reference points periodically transmitted their localization information [7], [16] since, (a) the sensor do not need to wait till the next beacon transmission to estimate their position, and (b) reference points need not make unnecessary transmission when nearby sensors have not moved.

The feature of sensor initiated localization is secured via the use of a pairwise key between the sensor and the communicating locator. Though at a first glance it seems that the requirement for a pre-deployed pairwise key between each sensor and each locator poses a scalability problem in terms of key storage and required communication, we can argue that this extra overhead is distributed among the locators which have higher energy resources, while minimal communication is required by the sensors.

To give an example of the scalability of our algorithm consider that 800 locators are randomly deployed within an area of $\mathcal{A} = 4km^2$ ($\rho_L = 2 \cdot 10^{-4}$ locators/m^2), and have a communication range $R =$ 100m. For such a deployment each sensor is able to hear on average $\rho_L \pi R^2 = 6.28$ locators. Consider also that sensors are randomly deployed within the same area $\mathcal{A}$, with a sensor density $\rho_s = 0.02$ sensors/m^2 that corresponds to 80,000 sensors being deployed. If the sensor communication range is $r = 10m$ each sensor is able to communicate on average with $\rho_s \pi r^2 = 6.28$ sensors, which is a minimum requirement to achieve network connectivity [13]. For the network of 80,000 sensors covered only by 800 locators, each locator communicates on average with $\rho_s \pi R^2 = 628$ sensors. Hence, the communication cost of ROPE for the foreseeable sensor network sizes (at best a few thousands) does not pose a scalability problem.

IV. SECURITY ANALYSIS

A. Attacker model

We assume that the attacker attempts to spoof the location of the sensors, i.e. force the sensors to estimate a location significantly different than their real location. We also assume that the attacker has to remain undetected in its effort to spoof the locations of the sensors. Hence, the attacker does not prevent the sensors from making any location estimation. Sensors that cannot estimate their location, detect that they are under attack and are excluded from the network, since they cannot associate a location with their monitoring data.

Furthermore, we assume that the attacker is capable of selectively jamming any transmission, thus denying communication between any network entities at will. The attacker can jam specific transmissions by blocking specific frequencies, and/or performing directional transmissions towards the transmitter/receiver that needs to be blocked. However, we assume that the attacker does not jam all beacons with a high power omnidirectional transmission. Such an attack would lead to a Denial of Service (DoS) and essentially prevent any network communication, thus. making the task of localization impossible.

B. Maximum spoofing impact

To quantify the impact of each type of attack and classify the adversaries based on their ability to spoof the locations of the sensors, we introduce a new metric called *Maximum Spoofing Impact* (MSI). Let SR denote the union of all the regions where the sensor can be spoofed to estimate its position due to an attack. The Maximum Spoofing Impact metric is defined as the maximum of all distances between the actual position of the sensor and the points in SR,

$$MSI = \max_{p \in SR} \|p - s\|. \qquad (8)$$

C. Wormhole Attack – Replaying beacons

Threat model: The wormhole attack is a replay type of attack [11], where the adversary records information at one (or multiple) point(s) of the network, referred as the *origin point*, tunnels it via a direct wired link or long range wireless transmission to another point of the network, referred as the *destination point*, and replays the information. The wormhole attack does not compromise the integrity and authenticity of the communication [11], and hence security primitives that ensure integrity and source authentication such as Message Authentication Codes, do not detect the attack.

Wormhole attack against ROPE: An adversary launching a wormhole attack against the localization procedure, provides to sensors false location information. In ROPE, the adversary can replay beacons originating from locators that are at a remote site compared to the sensor's real position.

When the sensor broadcasts its Id_s along with a nonce N_s, the attacker records the message, tunnels it to some distant point of the network and replays the message. In the next step, locators reply with
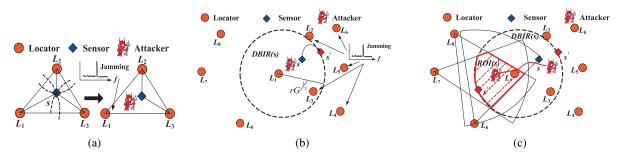
Fig. 5. (a) The attacker prevents sensor s from performing verifiable multilateration by jamming one of L_1, L_2, L_3, or enlarging the distance of s from L_3, (b) the attacker jams all transmissions from locators $L_2 \sim L_5$ and enlarges the distance from s to L_1 in order to enlarge the $DBIR(s)$ to the maximum possible region, (c) the attacker replays beacons from locators L_1, L_5, L_6, L_8 to displace the sensor in $ROI(s)$ with the MSI occurring at s''.

localization information and the attacker records the beacons tunnels them back to the sensor's position and replays them to the sensor. Note that the attack has to be performed in a timely manner, before the nonce N_s broadcasted by the sensor expires.

Let LH_s^r denote the set of locators replayed at the sensor s under attack, and assume that s can perform VM i.e. is included within a triangle $\triangle L_i L_j L_k$. Assume also that the attacker has enlarged the distance from s to L_i by jamming the transmission of L_i and replaying the message of L_i, after some delay. Since the sensor can perform VM, it still has to be inside $\triangle L_i L_j L_k$. However, since the distance to L_i is now enlarged, at least one of the distances to L_j, L_k has to be reduced, which is not possible due to distance bounding. Hence, the attacker cannot spoof the location of a sensor, when the sensor can perform VM.

However, the adversary can prevent the sensor from performing VM by jamming the signals from $L_i \in LDB_s$ so that no triangle exists that includes the sensor. In Figure 5(a), the sensor s is included inside $\triangle L_1 L_2 L_3$, and hence could possibly perform VM. An attacker jams locator L_1, so that s is not included within any triangle.

If the sensor cannot perform VM, the attacker can displace the sensor only within the $DBIR$. The maximum spoofing impact occurs in the scenario illustrated in Figures 5(b),(c). In Figure 5(b), the adversary jams all signals from the set LH_s, but the locator L_1 (if L_1 was also jammed the sensor would not be able to localize itself and the attack would be detected). The sensor performs distance bounding with L_1, but the adversary enlarges the distance to the maximum allowable distance of $rG^{\frac{1}{\gamma}}$. Hence, the sensor defines the $DBIR(s)$ as the disk of radius $rG^{\frac{1}{\gamma}}$, centered at L_1.

In Figure 5(c) the attacker records beacons from locators L_1, L_6, L_7, L_8 (L_6, L_7, L_8, are within the range of L_1), tunnels them via the wormhole link and replays them in the proximity of s. The sensor computes the $ROI(s)$ as the intersection of $DBIR(s)$ with $\cap_i S_i, i = \{1, 6, 7, 8\}$. The Maximum Spoofing Impact (MSI) that the attacker can cause based on this type of attack is

$$MSI = \|s - L_i\| + rG^{\frac{1}{\gamma}}, \qquad (9)$$

where L_i is the locator in LDB_s that is not jammed.

Note that the adversary needs significant resources (knowledge of the position of sensors and locators, wormhole link, jamming of multiple transmissions) to spoof the location of just one, or a small set of sensors, at best by MSI. In order to spoof the location of many sensors, the adversary needs to repeat the attack by jamming different locators and replaying beacons from different sets of locators. Hence, the cost of the attack becomes prohibitive in comparison to the impact of a limited displacement of very few sensors of the network.

D. Sybil attack – Impersonating network entities

In a Sybil attack [8], [17], the adversary performs node impersonation by either generating valid node identities, or assuming the identities of existing nodes. In ROPE, sensors do not rely on other sensors to estimate their location. Hence, an attacker has no incentive to impersonate sensors. On the other hand, an attacker can inject bogus localization information into the network if it is able to impersonate locators.

In order for an attacker to impersonate a locator L_i to a sensor s, the attacker must be able to generate a valid message authentication code (MAC) for the bogus beacon information. However, it is computationally infeasible for an attacker to find M', K' such that $MAC_{K'}(M') = MAC_{K_{L_i}^s}(M_i^k)$. Furthermore, only locator L_i has knowledge of the pairwise key $K_{L_i}^s$ besides the sensor s. Hence, an attacker cannot impersonate a locator L_i, unless it compromises L_i. We describe node compromise in the following section.

E. Compromised network entities

A network entity is assumed compromised if an adversary gains access to all its cryptographic quantities. In ROPE, the compromise of a sensor reveals nothing more than the pairwise key of the compromised sensor with each locator. Since sensors do not assist other sensors in localization, their compromise cannot facilitate location spoofing.

Though locators are assumed to be significantly more difficult to compromise, ROPE is impacted by any such compromise. The combination of locator compromise with the attacker's ability to jam any transmission desired, constitutes a severe security breach. The attacker gains access to all the pairwise keys between the compromised locator and each sensor. Hence, the adversary can perform distance bounding with any sensor and generate valid MACs for any bogus localization information.

To mitigate the impact of a single locator compromise, we can require to involve more than one locator in the location determination scheme. Based on the statistics of our locator deployment, we can compute the probability of a sensor to perform distance bounding with k locators (see Section V). Hence, we can require each sensor to perform distance bounding to at least k_{min} locators in order for its location estimation to be valid. The adversary has to compromise at least k_{min} locators in order to spoof the location of sensors. The increase of the resilience of ROPE in locator compromise, comes at the expense of increased locator density, since the sensor must be able to communicate with at least K_{min} locators. It is evident that if a fraction of the locators (reference points) are compromised and the attacker can control the information flow to the sensors via jamming, impersonation and selective replay, providing a robust
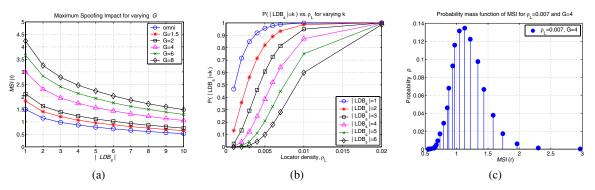
Fig. 6.   (a) Maximum Spoofing Impact (MSI) vs. the number of locators $|LDB_s|$ that a sensor s can bi-directionally communicate with, for varying antenna directivity gain G at the locator, (b) probability that a sensor s can bi-directionally communicate with $|LDB_s|$ locators, vs. locator density ρ_L, for $G = 4$, (c) the probability mass function (pmf) of MSI, for $\rho_L = 0.007$ and $G = 4$.

position estimation is a very difficult task.

V. PERFORMANCE EVALUATION

In this section we evaluate the resilience of ROPE against attacks in WSN, via simulations. We show that ROPE "ties" each sensor around a set of locators thus limiting the possible sensor displacement.

A. Simulation setup

For our simulations, we randomly placed 5,000 sensors within a square area of size $100m \times 100m$ ($\rho_s = 0.5$ sensors/m^2), and also randomly placed locators within the same area with varying density ρ_L. We set the sensor-to-sensor communication range to $r = 4m$, and the locator-to-sensor communication range $R = 20m$, when locators use omnidirectional antennas. The communication range R is adjusted based on the directivity gain G when directional antennas are used at the locators. Each sensor communicates with $\rho_s \pi r^2 = 6.28$ sensors on average, while it hears $\rho_L \pi R^2$ locators on average.

In our simulations we evaluate the Maximum Spoofing Impact under different deployment scenarios to illustrate the robustness of ROPE against different types of attacks. Due to space limitations we do not provide an analysis of the performance of ROPE in a benign environment when no attacks occur and all beacons are available at each sensor. Naturally, in a trusted environment the localization accuracy achieved is significantly higher than when localization information is blocked due to jamming, or other type of attacks.

B. Maximum spoofing impact vs. locator density.

In Section IV, we showed that if an adversary jams all locators but one, the MSI is equal to (9). In our first experiment, we evaluate the MSI that an adversary can achieve, if it has full knowledge of the network topology i.e. the positions of both the sensors and the locators of the network, but does not jam locators from the set LDB_s. Instead the adversary enlarges the distance bounds to the maximum value of $r_{sL} = rG^{\frac{1}{\gamma}}$. For each sensor, we compute the Distance Bound Intersection Region ($DBIR$) based on the enlarged distance bounds and evaluate the MSI as the longest distance between the actual position of the sensor and any point of the $DBIR$,

$$MSI = \max_{p \in DBIR} \|s - p\|. \qquad (10)$$

In Figure 6(a), we show the MSI in units of sensor communication range r vs. $|LDB_s|$ for varying antenna directivity gain G at the locator. We observe that the MSI decreases with the increase of $|LDB_s|$, as the sensor is able to bound its distance to multiple locators. On the contrary, the increase of the antenna directivity gain

G increases MSI, since the sensor is able to communicate with locator at longer distances and hence, the $DBIR$ grows larger.

Since MSI is a function of $|LDB_s|$, we can derive the statistics on MSI based on the statistics of LDB_s. The probability that a sensor communicates with $|LDB_s| = k$ locators is computed via *Spatial Statistics Theory* [5]. The random deployment of sensors and locators can be modeled after a Homogeneous Poisson Point process [5], with rates ρ_s and ρ_L, respectively. Hence, we can express the probability that a randomly deployed sensor can communicate with k locators as [16]:

$$P(|LDB_s| = k) \quad 1 - e^{-\rho_L \pi r^2 G^{\frac{2}{\gamma}}} \quad . \qquad (11)$$

In Figure 6(b), we show the probability $P(|LDB_s| = k)$ vs. the locator density ρ_L, for different values of k, and for $G = 4$. For example, when $\rho_L = 0.007$, a sensor bi-directionally communicates with four locators with a probability $P(|LDB_s| = 4) = 97.55\%$, while it communicates with six locators with a probability $P(|LDB_s| = 6) = 87.14\%$. Note that for $\rho_L = 0.007$, we only need 70 locators to cover a deployment region of 100x100.

Based on Figures 6(a),(b), we can compute the probability distribution for the MSI, for given values of ρ_L, G. In Figure 6(c), we show the probability mass function (pmf) of MSI for $\rho_L = 0.007$ and $G = 4$. We show the distribution of MSI as discrete, since MSI depends on $|LDB_s|$ that takes only discrete values. In fact since $|LDB_s|$ is distributed according to a Poisson distribution, we observe that the pmf of MSI is also Poisson distributed.

C. Locator density requirements

If a sensor is able to perform VM, spoofing a location inside the $DBIR$ can be avoided. To do so, a sensor s must be included within at least one triangle formed by three locators of the set LDB_s. In Figure, 7(a), we show the probability $P(VM)$, that a sensor s is able to perform verifiable mulitlateration vs. $|LDB_s|$. We observe that as $|LDB_s|$ increases, the probability that the sensor is included within a triangle formed by three locators in LDB_s also increases. Note that $P(VM)$ is independent of the antenna directivity gain G, for a given value of $|LDB_s|$, since whether the sensor is inside a triangle of locators is only dependent upon $|LDB_s|$ and not how far or close those locators are positioned. However, higher directivity gain G implies that a greater number of locators will be able to perform VM with each sensor assuming constant transmission power.

In Figure 7(b), we show the percentage of sensors able to perform verifiable multilateration vs. the locator density ρ_L, for varying G. As expected, the number of sensors able to perform multilateration,
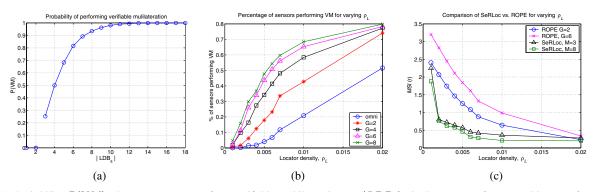
Fig. 7. (a) Probability $P(VM)$, that a sensor can perform verifiable multilateration vs. $|LDB_s|$, (b) Percentage of sensors able to perform verifiable multilateration vs. ρ_L for varying G, (c) comparison of ROPE with SeRLoc for varying locator densities.

grows with the locator density and the antenna directivity gain G. For higher locator density, the sensors perform distance bounding with more locators and hence, according to Figure 7(a) there is a higher chance that they can perform verifiable multilateration. Similarly for higher directivity gain G, the sensors are able to perform distance bounding with locators further away. Hence, for the same ρ_L but higher G, sensors perform distance bounding with more locators and a higher percentage performs verifiable multilateration.

In Figure 7(c), we compare the MSI achieved by ROPE with the MSI of SeRLoc presented in [16], for varying locator densities. We observe that as the density increases the performance of the two algorithms becomes identical. However, the MSI for SeRLoc is shown when jamming is not feasible. If jamming is present an attacker can spoof any location. Compared to SPINE presented in [7], ROPE can limit the MSI even for very low densities. In [7], a much higher locator density is required to allow sensors to perform VM as shown Figure 7(b).

VI. CONCLUSION

We studied the problem of secure position determination and location verification in wireless sensor networks. We proposed a sensor initiated localization algorithm called Robust Position Estimation (ROPE), that achieves robust sensor localization and verification of sensor location claims even in the presence of malicious adversaries. Compared to previously proposed schemes, ROPE allows sensors to estimate their own location without the assistance of a central authority, while being resistant to severe types of attacks such as the wormhole attack, node impersonation and jamming of transmissions. We introduced a new metric called Maximum Spoofing Impact (MSI) for evaluating the impact of possible attacks, and showed that ROPE limits the MSI even for low densities of reference points.

ACKNOWLEDGMENTS

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] 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.

[4] 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.

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

[6] 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.

[7] S. Čapkun, J. Hubaux, Secure Positioning of Wireless Devices with Application to Sensor Networks, to appear in *Proceedings of INFOCOM,* Miami, FL, USA, March 2005, available to the reviewers upon request.

[8] J. Douceur, The Sybil Attack, In *Proceedings of IPTPS 2002,* Cambridge, MA, USA, March 2002.

[9] R.J. Fontana, E. Richley, and J. Barney, Commercialization of an Ultra Wideband Precision Asset Location System. In *Proceedings of IEEE Conference on Ultra Wideband Systems and Technologies,* Nov. 2003.

[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] 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.

[12] M. Kuhn, An Asymmetric Security Mechanism for Navigation Signals, In *Proceedings of the 6th Information Hiding Workshop,* May 2004, Toronto, Canada.

[13] L. Kleinrock, and J. Silvester, Optimum Transmission Radii for Packet Radio Networks or Why Six is a Magic Number, In *Proceedings of IEEE National Telecommunications Conference,* 1978, pp. 4.3.1-4.3.5.

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

[15] Mica wireless measurement system. In http://www.xbow.com/Products/ Product_pdf_files/ Wireless pdf/MICA.pdf.

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

[17] J. Newsome, E. Shi, D. Song and A. Perrig, The Sybil Attack in Sensor Networks: Analysis and Defenses, In *Proceedings of IPSN,* Berkeley, CA, April 2004.

[18] 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.

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

[20] N. Sastry, U. Shankar and D. Wagner, Secure Verification of Location Claims, In *Proceedings of WISE,* San Diego, CA, USA, Sept. 2003.

[21] 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.

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