Open access • Proceedings Article • DOI:10.1109/INFOCOM.2006.302

Secure Localization with Hidden and Mobile Base Stations — Source link

Srdjan Capkun, Mario Cagalj, Mani Srivastava

Institutions: Technical University of Denmark, École Polytechnique Fédérale de Lausanne, University of California, Los Angeles

Published on: 23 Apr 2006 - IEEE International Conference Computer and Communications

Topics: Mobile computing, Base station, Wireless network and Radio frequency

Secure Localization With Hidden and Mobile Base Stations

Srdjan Čapkun
Informatics and Mathematical Modelling Department
Technical University of Denmark (DTU)
DK-2800 Lyngby, Denmark
sca@imm.dtu.dk

Mario Čagalj
School of Computer and Communication Sciences
Ecole Polytechnique Fédérale de Lausanne (EPFL)
CH-1015 Lausanne, Switzerland
mario.cagalj@epfl.ch

Mani Srivastava
Networked & Embedded Systems Laboratory (NESL)
Electrical Engineering Department
University of California
Los Angeles, CA, 90095
mbs@ucla.edu

***Abstract*— Until recently, the problem of localization in wireless networks has been mainly studied in a non-adversarial setting. Only recently, a number of solutions have been proposed that aim to detect and prevent attacks on localization systems. In this work, we propose a new approach to secure localization based on hidden and mobile base stations. Our approach enables secure localization with a broad spectrum of localization techniques: ultrasonic or radio, based on received signal strength or signal time of flight. Through several examples we show how this approach can be used to secure node-centric and infrastructure-centric localization schemes. We further show how this approach can be applied to secure localization in sensor networks.**

I. Introduction

In the last decade, researchers have proposed a number of positioning and ranging techniques for wireless networks [43], [44], [35], [3], [20], [7]. The use of these techniques is broad and ranges from enabling networking functions (i.e., position-based routing) to enabling location-related applications (e.g., access control, data harvesting).

The proposed techniques were mainly studied in non-adversarial settings. Ranging and positioning techniques are, however, highly vulnerable to attacks from dishonest nodes and external attackers; dishonest nodes can report false position and distance information in order to cheat on their locations; external attackers can spoof measured positions of honest nodes. Positioning and ranging techniques in wireless networks mainly rely on measurements of the times of flight of radio (RF ToF) or ultrasound signals (US ToF), and on the measurements of received strengths of radio signals of devices (RF RSS). An attacker can generally influence all these measurements by jamming and delaying signals, and by modifying their signal strengths. Positioning systems based on ultrasound time of flight (US ToF) and those based on measurements of signal strength of radio signals (RF RSS) are particulary vulnerable to position spoofing attacks. Systems based on radio time of flight measurements are less vulnerable to attacks because of the high speed of signal propagation,

Recently, a number of secure positioning techniques were proposed [25], [26], [10], [28], [29] to cope with these problems. These mechanisms rely on GPS, high speed hardware, directional antennas, or on robust statistics.

In this paper, we propose a different approach to secure positioning that relies on a set of covert base stations used for secure positioning. By covert base stations (CBS), we mean base stations whose positions are not known to the attacker at the time of the execution of secure positioning. In our system, positions of covert base stations represent a secret input *(a key)* to the system. Covert base stations can be realized by hiding or disguising static base station or by the random motion of mobile base stations. Typically, covert base stations are passive.

We show through three example protocols how covert base stations can be used to secure node-centric and infrastructure-centric positioning, as well as positioning in sensor networks. We discuss how security of the proposed protocols depends on the precision of the positioning and ranging techniques, and on the number of the covert base stations. We capture this analytically.

The organization of the rest of the paper is as follows.

In Section II, we present our system model. In Sections III and IV we present protocols for secure positioning in infrastructure-centric and node-centric systems, respectively. In Section V, we show how mobile base stations can be applied to secure positioning in sensor networks. In Section VI, we analyze our schemes. In Section VII, we overview the related work. We conclude the paper in Section VIII.

II. Model

In this section, we describe our system and attacker models.

A. System model

Our system consists of a set of covert base stations (CBS) and a set of public base stations (PBS) forming a positioning infrastructure. Here, by covert base stations we mean those base stations whose positions are known only to the authority controlling the verification infrastructure. To prevent that their positions are discovered through radio signal analysis, covert base stations are silent on the wireless channel; they only listen to the on-going communication.

In our system covert and public base stations know their positions or can obtain their positions securely (e.g., through secure GPS [25]). Here, we assume that the attackers cannot tamper with these positions nor compromise the base stations.

We also assume that every legitimate node shares a secret key with the base stations, or that base stations hold an authentic public key of the node. This key is established/obtained through the authority controlling the verification infrastructure prior to position verification. Here, all communication between the authority and a node is performed through a public base station, whereas the hidden stations remain passive.

We further assume that covert base stations can measure received signal strength or have an ultrasound interfaces through which they perform ranging.

In most of this work, we assume that covert base stations are static. Thus, their mutual communication and their communication to the verification authority is performed through a channel that preserves their location privacy; this communication channel is typically wired (or infrared), such that they cannot be detected by the attackers. In Section V, we modify our assumptions and we assume that the base stations are mobile, and that their mutual communication is wireless.

B. Attacker model

We observe two types of attacks: internal and external. Internal attacks are those in which a dishonest or compromised node (internal attacker) reports a false position or convinces the positioning infrastructure that it is at a false position. External attacks are those in which an external attacker convinces an honest node and the positioning infrastructure that the node is at a different position from its true position (i.e. the attacker *spoofs* node's position).

We observe two types of positioning systems: node-centric and infrastructure-centric. By a node-centric positioning system, we mean that a node computes its position by observing signals received from public base stations with known locations. If the positioning system is *node-centric*, internal attacks are generally straightforward; a the attacker simply lies about the position that it computed. *Infrastructure-centric* positioning systems are those in which the infrastructure computes positions of nodes based on their mutual communication. In multilateration-based approaches, an internal attacker can cheat on its position by cheating on ranging mechanisms (i.e. by reporting false signal strengths and times of signal sending/reception). In time difference of arrival (TDOA) systems, an attacker can cheat by sending signals to base stations at different times (in some cases, the attacker would need to have directional antennas).

Attacks by external attackers are similar to those performed by internal attackers. An external attacker can perform timing attacks by delaying (through jamming) or speeding-up (wormhole attacks [22]) the signals, or can performs power level modification attacks by changing the power levels at which nodes and the base stations transmit.

In this attacker model, we assume that the attackers know the positions of the public base stations and thus can modify computed ranges and time differences such that they are consistent with the false position.

III. Infrastructure-centric positioning with hidden base stations

In this section, we describe a simple solution for securing infrastructure-centric positioning systems, based on time difference of arrival (TDOA) and covert base stations.

TDOA is the process of positioning a source of signal in two (respectively three) dimensions by finding the intersection of multiple hyperbolas (or hyperboloids) based on the time difference of arrival between the

signal reception at multiple base stations. An hyperboloid is defined as a surface, that has a constant distance difference from two points (in our case two base stations). Using two hyperbolas (three base stations) we can obtain two dimensional device positions, and using three hyperboloids (four receivers) we can determine three dimensional positions. The operation of the TDOA technique is shown on Figure 1. Node A sends a radio signal, and the verifiers measure the difference between the times t_1, t_2, t_3, t_4 of the signal reception at each verifier and determine the position of A.

One of the main advantages of TDOA is that node positioning does not require communication from the base stations to the mobile nodes: the base stations locate mobile nodes measuring signal reception times at each base station. This is why TDOA is well suited for secure positioning with hidden base stations.

In our protocol, the base stations are hidden, and only listen to the beacons sent by the nodes. Upon receiving the beacons, the base stations compute node's location with TDOA, and check if this location is *well consistent* with the time differences. By well consistent we mean that the computed position is not to far from the hyperbolas constructed with measured time differences (Figure 1). TDOA with hidden base stations is designed to detect both internal and external attacks, and relies on the assumption that the attackers can guess the positions of base stations only with a very low probability. The protocol is executed as follows.

TDOA with hidden base stations

1 $PBS(t_s) \rightarrow A: \ N$

2 $A \rightarrow *: \ \mathrm{m} = \{A, N, \ \mathrm{sig}_{K_A}(A, N)\}$

3 CBS_n : receive m at t_r^n

: with $t_r^1, ..., t_r^n$, compute p with TDOA

: if $\sum_{i>j}(|t_r^i - t_r^j| - h(p,i,j))^2 \leq \Delta$ and $\max_i(t_r^i - t_s) \leq T$

then $p_A = p$; else reject p

Here, p is a position of node A computed from the measured time differences and it is the solution to the following least-square problem:

$$p = \arg\min_{p^*} \sum_{i>j} (|t_r^i - t_r^j| - h(p^*, i, j))^2$$

where $h(i, j, p^*)$ is the difference of signal reception times at CBS_i and CBS_j, if the signal is sent from position p^*. Δ is the maximal expected inconsistency between the computed position and the measured time differences. This inconsistency is caused by the errors in measurements of reception times and by pair-wise clock

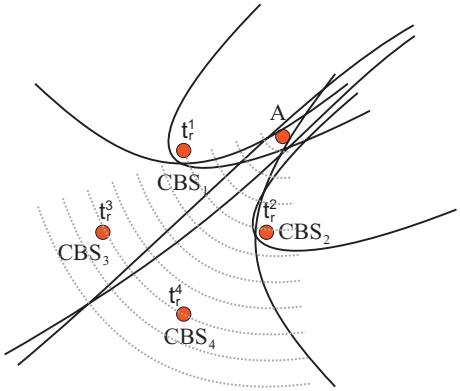

Fig. 1. An example of positioning with Time Difference Of Arrival. The base stations CBS measure the differences of signal arrival times, and compute the position of node A.

drifts of the base stations. T is the time within which a node needs to reply to a challenge issued by a public base station; this response time is important for the prevention of some replay attacks and to ensure message freshness. N is a fresh nonce. Note that the covert base stations know which nonce is sent by the public station.

A. Security analysis

Conventional TDOA schemes are vulnerable to both internal and external attacks. An internal attacker can send messages to base stations, with appropriate delays (potentially using directional antennas) and thus cheat on its location; external attackers can jam and delay node's original messages and thus spoof its location.

With covert base stations, these attacks are prevented; to successfully cheat, the attackers need to know where the base stations are located. Otherwise, the attacker needs to guess the locations of the base stations, and perform appropriate timing attacks. The attacker's cheating success depends on the system precision Δ. Essentially, Δ defines the size of attacker's guessing space. Simply, if Δ is large, a false position will be more likely accepted, as the tolerance to inconsistencies will be higher. In Section VI, we investigate in more detail the dependence of attacker's success on Δ.

In addition, we need to consider one more external attack to TDOA. This attack is performed as follows: (1) Attacker jams the original positioning message (m) sent by node A; (2) Attacker replays m from a location p'_A. As a result, the base stations will be convinced that the node A is located at p'_A, whereas its true position is p_A. In order to mount this attack, an attacker needs to be able to jam all hidden base stations, which without knowing where they are located requires a lot of power

and resources. Furthermore, the attacker needs to have faster processing at nodes than regular mobile nodes. Finally, in order to show that the node A is at p'_A, the attacker needs to have access to this location. Still, this attack is feasible for a resourceful attacker.

Using covert base stations, this attack is partially prevented by the challenge-response scheme. In our protocol, the node is expected to reply to a challenge nonce N within a period T, which limits the time during which the attacker can mount the attack. Here, T is estimated based on the expected signal propagation times and node processing time. We note that if our simple challenge-response scheme is replaced by a more efficient distance-bounding protocol, this and similar attacks can be completely prevented. In some implementations, this will require some specialized hardware at the side of nodes and base stations [5]. The same attacks can also be prevented through precise time synchronization.

In our protocol, node location privacy is not preserved. However, this protocol can be enhanced to include public base station authentication which prevents an attacker from challenging the node and from requesting from it to send positioning signals disclosing its location. Other attacks are possible on node's location privacy [36], [19], [37], [40], [23], [24], but coping with these attacks is out of the scope of this paper.

IV. Node-centric positioning with hidden base stations

In this section, we present a protocol for secure positioning in node-centric positioning systems. Here, we assume that the node computed its position through a non-secure positioning system. This position is then reported to the infrastructure comprised of covert base stations, which then verifies if the position is correct. In this context, internal attacks are related to nodes lying about their locations, whereas external attacks are more complex, and assume that the attacker spoofs node's position and then cheats on the position verification mechanisms.

To cope with these attacks, we propose a *position verification* protocol that relies on hidden base stations. In this protocol, node A reports a position p_F to CBS. CBS then measures its distance d_F^m to the node (passively) and verifies if the reported position p_F corresponds to the measured distance. Our protocol is executed as follows (assuming that the distance between the CBS and the node is measured using ultrasound):

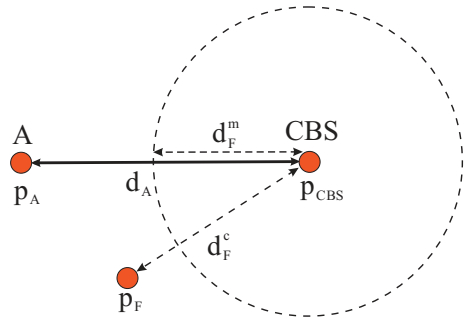

Fig. 2. False position report by node A to the covert base station. p_A is the true node position, p_F is the fake node position (reported by A to CBS), p_{CBS} is the position of CBS. $d_F^c = d(p_F, p_{CBS})$ is the (false) distance between CBS and A, computed by CBS, d_F^m is the (false) distance between A to CBS measured passively by CBS. If $|d_F^c - d_F^m| \leq \Delta$, then $p_A = p_F$.

Position verification with hidden base stations

1 $PBS(t_s) \rightarrow A: \ N$

2 $A \rightarrow$ (rf)$*: \ m_{rf} = \ p_F, \ \text{sig}_{K_A}(\text{rf}, p_F, N)$

(us) : $m_{us} = \ p_F, \ \text{sig}_{K_A}(\text{us}, p_F, N)$

3 CBS : receive m_{rf} at t_{rf} and m_{us} at t_{us}

: $d_F^c = d(p_F, p_{CBS})$

: $d_F^m = (t_{us} - t_{rf})s$

: if $|d_F^c - d_F^m| \leq \Delta$ and $(t_{rf} - t_s) \leq T$ then $p_A = p_F$; else reject p_A

Here, N is a nonce generated by the public base station, Δ is a combined positioning and ranging error and T is the time within which a node needs to reply to a challenge issued by a public base station.

In this protocol, the infrastructure uses a public base station to communicate with the node, and a single covert base station to verify the reported position. PBS sends a challenge to the node A, which then replies by sending a radio and an ultrasound messages, containing the alleged node position p_F. CBS then measures the time difference between the time at which it received the radio signal (t_{rf}) and the time at which it received the ultrasound signal (t_{us}), and computes the distance $d_F^c = d(p_F, p_{CBS})$ to A. If the reported (possibly fake) position corresponds to the measured (possibly fake) distance, CBS concludes that p_F is the position of A. To do this, CBS simply computes the distance $d_F^c = d(p_F, p_{CBS})$ between its own position p_{CBS} (which is unknown to the node) and the reported position p_F and compares it with the measured distance d_F^m (which A can enlarge or reduce). If two distances differ by more than the expected combined positioning and ranging error Δ, then the position is rejected; else, the position is accepted as true node position. An additional verification is made

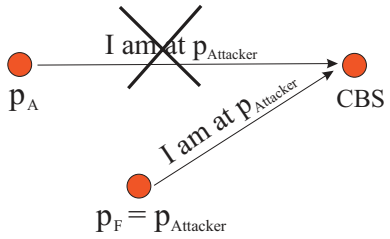

Fig. 3. Position spoofing attack. Attacker spoofs node A and CBS into believing that it (the node) is at its (attacker's) position p_F. The attacker then replays node's message from p_F to fool the position verification mechanism.

by measuring the node response time T, in order to prevent replay attacks.

We note that this protocol could be similarly designed with RF RSS-based ranging techniques.

A. Security analysis

An internal attack in node-centric positioning schemes is simply a false position report from the node to the infrastructure. Our protocol detects false position reports through checking the consistency of the reported position and of the measured distance. This detection mechanism relies on the fact that the attacker can guess the distance of p_F to the hidden base station only with a low probability. We analyze this in detail in Section VI.

External attacks against position verification are more complex and include position spoofing, jamming and message replays. Figure 3 shows an external attack on position verification. Node A is positioned at p_A, the attacker at position p_F. The attacker first spoofs the position of A such that A believes that it is positioned at p_F. Then, by replaying A's positioning signals (radio and ultrasound) from p_F, the attacker fools the position verification mechanism. This attack enables the attacker to convince the device A that it (A) is positioned at p_F and then convinces the covert base station that A is at p_F. One limitation of this attack is that an attacker needs to have a device at the position where it wants to falsely place A and that the attacker nodes need to be fairly synchronized to perform it.

Our position verification protocol partially prevents this attack by the same technique used in the TDOA protocol with hidden base stations; the base stations request that the node replies with the RF message to the PBS challenge within a time bound T. This limits the time within which the attacker can mount the attack. With distance-bounding techniques [5], this attack can be entirely prevented, as the value of T can be reduced to nanoseconds.

Similarly to our TDOA-based protocol, the position verification protocol is also vulnerable to location privacy threats. Here, the most obvious privacy problem is that the node discloses its position to any station that issues a position verification request (step 2 in the protocol). An attacker can simply listen to the node's messages and learn where the node is located. Similarly, an attacker could send a position verification request to the node to keep track of the nodes position. These attacks can be prevented by simply requiring a public base station to authenticate itself to the node, and by having a node encrypt the position information that it sends to the base stations.

V. Secure positioning in sensor networks with mobile base stations

The use of mobile base stations has already been proposed for data collection, energy preservation, localization and security in wireless networks [39], [11], [21]. Many mobile platforms have emerged as a result: Amigobot [1], Cotsbot [4], Millibot [31], Robomote [12], and Ragobot [17].

In this section, we describe the use of mobile base stations for secure positioning in static sensor networks.

A. Motivation

Knowing positions of sensors is essential for binding the measured data with the place at which it was measured. Without the position information, most sensor networks would be made useless. Because of this, a number of positioning systems have been proposed for sensor networks (see Section VII). However, most of these positioning systems were not designed with security in mind and are therefore vulnerable to attacks that can render the information that sensors measure useless. Recently, a number of secure positioning systems for sensor networks were proposed, based on robust statistics [28], [29], directional antennas [26] and/or distance bounding [10]. Here, we take a different approach and we rely on mobile base stations. We show how mobile base stations can be used to secure positioning and to verify the positions of sensor nodes.

B. Scenario

In our scenario, we assume that the sensors compute their positions through one of the non-secure positioning algorithms [13], [6], [9], [33], [32], [42], [30], [14], [8].

We further assume that the authority has a number of mobile base stations (similar to data mules), that know securely their locations (e.g., through secure GPS [25]).

These mobile base stations can be single-purpose or multi-purpose, and therefore can be used for only position verification or also for data collection and other tasks.

We assume that the mobile base stations share a secret key with each sensor.

C. Position verification with mobile base stations

The protocol presented in this section is similar to the position verification protocol presented in Section IV. That protocol relied on the assumption that the covert base station is hidden, whereas all communication between the node and the positioning infrastructure is performed through the public base station.

Here, position verification is performed through mobile base stations. This is realized such that the base station sends a verification request to the node from one location, and then waits for the response at a different location. Therefore, at the time of position verification, the node does not know the position of the mobile base station. In this protocol, the role of a public base station is thus replaced with base station mobility.

Our protocol is executed as follows:

Position verification with mobile base stations

1 (t_1) $MBS \rightarrow A:\ \mathrm{MBS}, N, T_R$

2 (t_2) $\mathrm{S} \rightarrow *\ (\mathrm{rf}):\ p,\ \mathrm{MAC}_K(\mathrm{rf}, p, \mathrm{MBS}, N)$

$(\mathrm{us}):\ p,\ \mathrm{MAC}_K(\mathrm{us}, p, \mathrm{MBS}, N)$

3 MBS : receive (rf) at t_{rf} and (us) at t_{us}

: $d_S^c = d(p, p_{MBS})$

: $d_S^m = (t_{us} - t_{rf})s$

: if $|d_1^c - d_1^m| \leq \Delta$ and $(t_{rf} - t_1) \leq T_R$

: then $p_S = p$; else reject p_S

Here, K is the secret key shared between the mobile station MBS and the sensor S; T_R is the time after which the sensor is suppose to send its reply (ideally, $T_R = t_2 - t1$). T_R is also an estimated time within which MBS will move to a location different from the one at which it was at t_1.

The operation of our protocol is illustrated on Figure 4. At time t_1 a mobile base station (MBS) is at position $p_{MBS}(t_1)$ and sends a message to the neighboring sensors containing a challenge nonce N and a time delay T_R after which the sensors needs to reply to the message. Within the time T_R, MBS moves to a different position $p_{MBS}(t_2)$ within the circle defined by its power range when it was at position $p_{MBS}(t_1)$. When at position $p_{MBS}(t_2)$, MBS receives a reply from those sensors which are still in its power range. Based on received replies, MBS computes the distances to the sensors and verifies their positions (this procedure is the same as in the position verification protocol presented in Section IV.

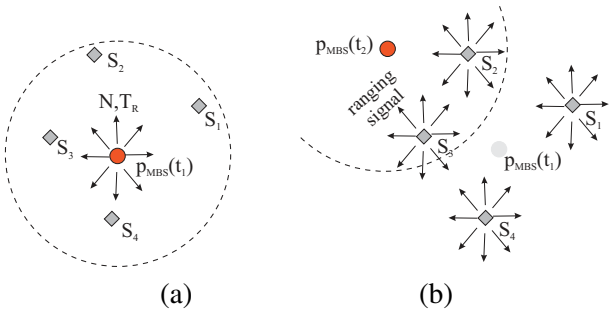

Fig. 4. Position verification in sensor networks. A mobile base station (MBS) verifies positions of nodes; (a) at time t_1 MBS challenges sensor nodes; (b) at time $t_2 > t_1$ the sensors reply to the challenge and their positions are verified by MBS.

Typically, the MBS can perform simultaneous verification of positions of multiple sensors. If MBS moves within the circle defined by its power range at time t_1, it will hear at least 39% of the sensors that were in its power range at time t_1, provided that the sensors are uniformly distributed over MBSs power range. This is because the intersection of MBSs power ranges at t_1 and at t_2 will be at least 39% of the circle surface, given that MBS moved within its previous power range. At time t_1 MBS broadcasted a challenge to the nodes, and at time t_2, the nodes replied. After position verification, MBS issues another challenge for the nodes in its power range whose positions were not verified; then, MBS moves again and waits for their reply. Hence, as MBS moves through the network, it will verify only positions of those sensors which were in the intersections of the two subsequent power ranges of MBS. This is illustrated on Figure 5. The trajectory of MBS needs to be unpredictable for the sensor nodes, even if the sensors collude. One way how to ensure this is to have MBSs move according to random walk. Given this, if the sensors are placed on a grid, the time in which the MBS covers the network can be estimated as $O(N \log N)$, where N is the number of sensors. In [39], [2], the authors provide a set of analytical and simulation results for coverage times of mobile stations on sensor grids.

Security and location privacy analysis of this protocol is very similar to the one of the position verification protocol presented in Section IV, and thus we do not repeat it here.

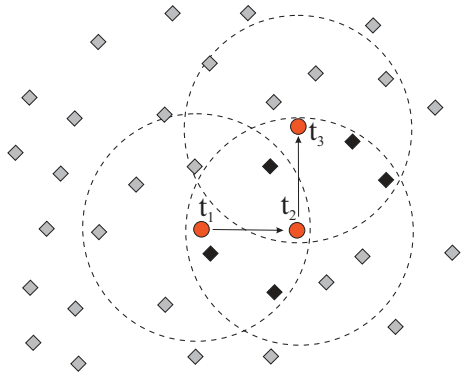

Fig. 5. Progress of position verification in sensor networks with mobile base stations. MBS moves from position $p_{MBS}(t_1)$ to $p_{MBS}(t_2)$ and $p_{MBS}(t_3)$.

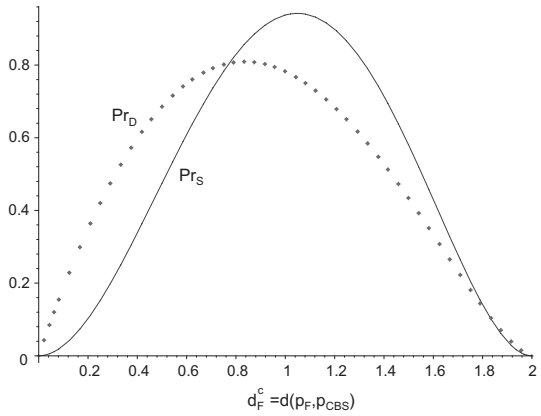

Fig. 6. Probability distribution function of the distance $d_F^c = d(p_F, p_{CBS})$ on a disk (Pr_D) and in a ball (Pr_S), when p_{CBS} and p_F are chosen uniformly over the disk and ball, respectively.

VI. Analysis

In this section, we analyze the likeliness that the attacker succeeds in cheating our secure position schemes by guessing the positions of the covert base stations. This probability will notably depend on the size of attacker's search space (which depends on base station power ranges) and on the precision of the positioning system.

Here, we focus on the position verification protocol described in Section IV. We define the attacker's success as an event when the attacker A reports a position p_F different from its true position ($p_F \neq p_A$), and the CBS concludes that $p_A = p_F$. This event will realize only if $|d_F^c - d_F^m| \leq \Delta$. This essentially means that for a chosen position p_F an attacker needs to guess the distance to the covert base station. The probability of attackers success is therefore

$$Pr(|d_F^c - d_F^m| \leq \Delta | p_F \neq p_A) \tag{1}$$

In our analysis we assume that the positioning takes place on a disk (2D), and in a ball (3D). The position of the hidden base station and the reported position of the attacker are therefore on a disk (or in the ball). We assume that the position of the base station is uniformly chosen on the disk (in the ball). Other geometries can be observed, but we have chosen the circles as they best reflect the power ranges of the devices.

A. Attacker's average success probability

To compute the average probability of attacker's success, we assume that the attacker chooses its fake position p_F uniformly over the disk/ball. In this case, the probability distribution function (pdf) of its distance to the uniformly chosen position of the hidden base station is given by [38]:

$$\begin{aligned} Pr_D(d_F^c = d) &= \frac{4d}{\pi R^2}\cos^{-1}(\frac{d}{2R}) \\ &\quad -\frac{2d^2}{\pi R^3}\sqrt{1-\frac{d^2}{4R^2}} \end{aligned} \tag{2}$$

for a disk and by

$$Pr_S(d_F^c = d) = \frac{3d^2}{R^3} - \frac{9d^3}{4R^4} + \frac{3d^5}{16R^6} \tag{3}$$

for a ball, where R is the radius of the disk/ball. Pr_D and Pr_S are shown on Figure 6. The maximum values of these functions are $Pr_D(d_F^c = 0.84R) = 0.809$ and $Pr_S(d_F^c = 1.05R) = 0.942$. This means that when the attacker guesses what is the length of $d(p_F, p_{CBS}$, it will have the highest chance of success if it guesses that it is 0.84R, and hence sets $d_F^m = 0.84R$. In this case, the probability of attacker's success will be:

$$Pr_{D,uni} = \int_{0.84R-\Delta}^{0.84R+\Delta} Pr_D d\mathrm{d} \approx 0.809 \times \frac{2\Delta}{R} \tag{4}$$

$$Pr_{S,uni} = \int_{1.05R-\Delta}^{1.05R+\Delta} Pr_S d\mathrm{d} \approx 0.942 \times \frac{2\Delta}{R} \tag{5}$$

These approximations hold for $\Delta << R$. These results are important as they show that the the probability of attacker's success grows linearly with the positioning and ranging error Δ and inversely proportional to radius of the region in which the hidden base station is places. This means that the probability of attackers success is inversely proportional to the square root of the space in which positioning is taking place. Simply, the more precise the positioning and distance measurement is,

and the larger the space is, the more secure is position verification.

The probability of attacker's success can be significantly reduced if multiple covert base stations are used for position verification. In that case, the probability of attacker's success is simply

$$Pr^n_{D,uni} \approx (0.809 \times \frac{2\Delta}{R})^n \quad (6)$$

$$Pr^n_{S,uni} \approx (0.942 \times \frac{2\Delta}{R})^n \quad (7)$$

The probability of attacker's success in both disk and ball can therefore be upper-bounded by $Pr^n_{uni} = (\frac{2\Delta}{R})^n$.

B. Attacker's maximum success probability

So far, we have assumed that the attacker chooses p_F uniformly, meaning that we have assumed that the position at which the attacker wishes to pretend to be can be anywhere within the disk/ball. Here, we observe what is position p_F, for which the attacker will have the highest probability of success. We show that the attacker has the highest probability of success ($Pmax$) if it chooses its fake position p_F at the center of the disk/ball and if it chooses $d^m_F = R$ as its fake measured distance to CBS. This probability is as follows (for disk):

$$\begin{aligned} Pr_D(d^c_F < d) &= \frac{d^2\pi}{R^2\pi} \\ Pr_D(d^c_F = d) &= \frac{\delta}{\delta d} Pr_D(d^c_F < d) \\ &= \frac{2d\pi}{R^2\pi} \\ Pmax_D = Pr_D(d^c_F = R) &= \frac{2}{R} \end{aligned} \quad (8)$$

Similarly for the ball, we obtain that $Pr_S(d^c_F = R) = \frac{3}{R}$. From this it follows that the maximum probabilities of the attacker's success $Pmax^n_D \approx (\frac{4\Delta}{R})^n$ and $Pmax^n_S \approx (\frac{6\Delta}{R})^n$. This analysis shows that in the worst-case scenario, the maximum probability of attacker's success is approx 2.5 times (disk, 2D) and 3 times (ball, 3D) the average probability of attacker's success (when $n = 1$).

Intuitive proof: It is sufficient to observe that the set with the highest number of points equidistant from a single point p in a disc/ball is the set of points on a circle (sphere) of radius R, when p is at the center of a disk/ball.

C. Further reducing the probability of attacker's success

Attacker's success can be further reduced by increasing the space in which the covert base stations can be positioned. So far we have assumed that the region in which the device proves its position (positioning region) is the same as the region within which the covert base stations are positioned. However, the covert base stations can be placed also outside of the positioning region (around the positioning region). The maximal distance of the covert base stations to the positioning region will depend on the power range of the attacker's device and on the antenna sensitivity of the base stations. This is illustrated on Figure 7. In this case, the maximum probability of attacker's success is further reduced from $Pmax_D \approx \frac{4\Delta}{R}$ and $Pmax_S \approx \frac{6\Delta}{R}$ to $Pmax'_D \approx \frac{4\Delta}{R'}$ and $Pmax'_S \approx \frac{6\Delta}{R'}$, respectively, as $R' > R$.

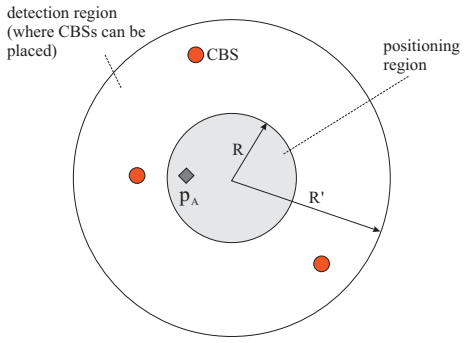

Fig. 7. Positioning and detection region. If the base stations can be positioned outside of the positioning zone, that the probability of the attacker's success can be further decreased.

This example further shows that regardless of the size of the positioning region (which can be arbitrarily small), the probability of attacker's success can be small if the detection region is sufficiently large.

D. Sensitivity

In this subsection, we analyze the frequency of false positives and false negatives as a function of the expected positioning and ranging error Δ. If the authority sets Δ to 0, the probability of the attacker's success will be 0, but due to the positioning and ranging errors the system will reject all reported positions, even if the device is not faking its position. In this case, the frequency of false negatives will therefore be 1. Similarly, if Δ is set to 2R (maximal distance in the positioning region of radius R), then the probability of the attacker's success will be 1 (if the reported position is in the center of the disk/ball). However, then, all the false positions of the attacker will be accepted and the frequency of false negatives will be 1. It is therefore important to set Δ such that it minimizes the false negatives and false positives. This means that Δ should be chosen as a minimum value that properly reflects positioning and ranging errors.

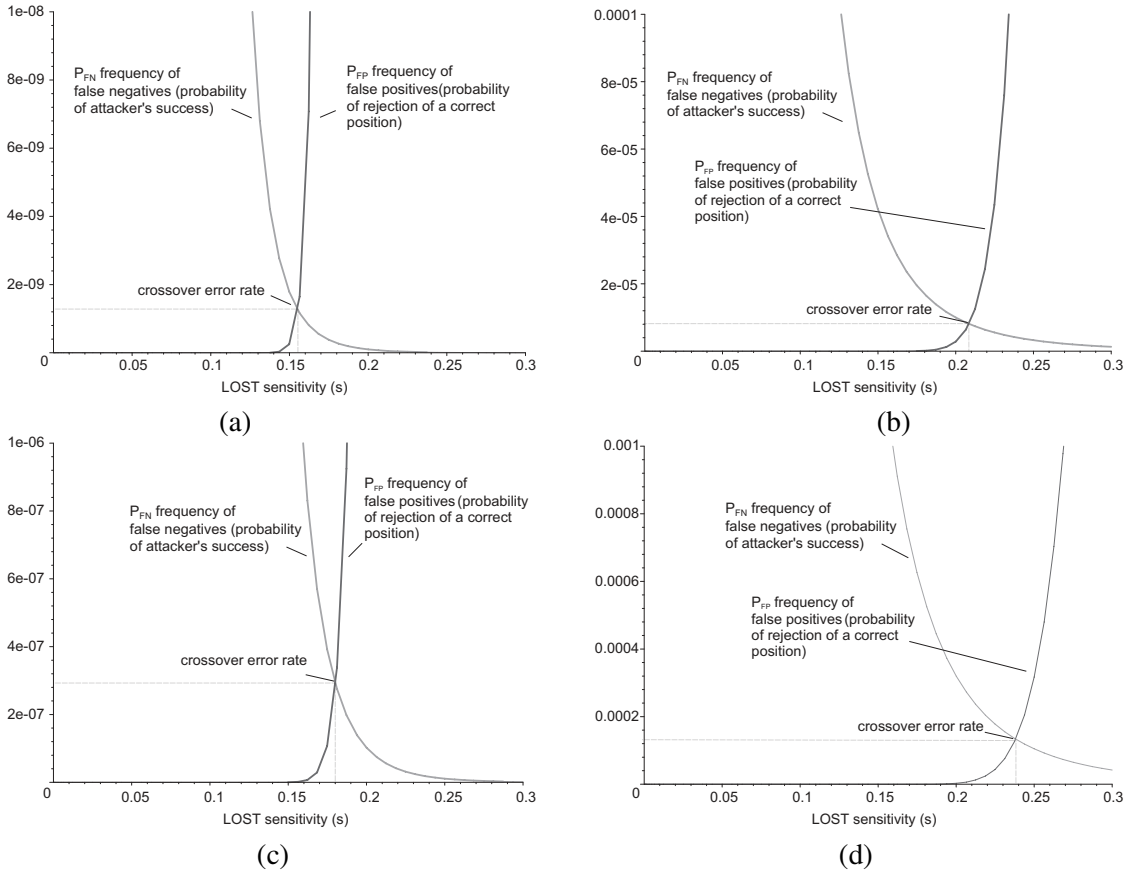

Fig. 8. The frequency of false positives and false negatives, and a crossover error rate for $\sigma = 0.005R, n = 10$ (a), $\sigma = 0.005R, n = 5$ (b), $\sigma = 0.01R, n = 10$ (c), $\sigma = 0.01R, n = 5$ (d). $s = 1/k$ is the sensitivity. $\Delta = k\sigma$ is the tolerated positioning and ranging error. σ is the standard deviation of the positioning and ranging error.

As we have already noted, CBSs accept the position of the node if $|d_F^c - d_F^m| \leq \Delta$. There are two sources of error in this system. The first error is the positioning error $error_P$, which is contained in the reported position p_F. The second error is the ranging error $error_R$ and it is contained in the distance measurement of d_F^m. The total error in $|d_F^c - d_F^m|$ is therefore $error = error_P + error_R$. If positioning and ranging errors are already known and if we can assume that they are gaussian $error_P \sim N(0, \sigma_P^2)$ and $error_R \sim N(0, \sigma_R^2)$ the the total error of $|d_F^c - d_F^m|$ is $error \sim N(0, \sigma^2 = \sigma_P^2 + \sigma_R^2)$. If the errors are non-gaussian or even not independent, then we do assume that the joint distribution of the $error$ can be obtained experimentally.

Without any loss of generality, we can express Δ in terms of σ as follows:

$$\Delta = k\sigma \tag{9}$$

where k is a positive real number and σ is the standard deviation of $error$ ($\sigma = \sqrt{\sigma_P + \sigma_R}$) for independent gaussian errors). In the case that $error$ is gaussian, the probability that $d_F^c - d_F^m$ falls within the interval $[-k\sigma, k\sigma]$ is given by [34]:

$$\begin{aligned} Pr(-k\sigma < d_F^c - d_F^m < k\sigma) &= \frac{2}{\sqrt{\pi}} \int_0^{\frac{k}{\sqrt{2}}} e^{-u^2} du \\ &= \operatorname{erf}(\frac{k}{\sqrt{2}}) \end{aligned} \tag{10}$$

Here, interval $[-k\sigma, k\sigma]$ is called the confidence interval. The frequency of false positives can be than computed as:

$$Pr_{FP} = 1 - Pr(-k\sigma < d_F^c - d_F^m < k\sigma) \tag{11}$$

i.e., as the probability that $d_F^c - d_F^m$ does not fall within the interval $[-k\sigma, k\sigma]$.

The frequency of false negatives is simply the probability of attacker's success given by (in 2D):

$$Pr_{FN} = \frac{4\Delta}{R} = \frac{4k\sigma}{R} \tag{12}$$

For n covert base stations, these probabilities are defined as follows. The frequency of false positives is defined as a probability that at least one of the covert base stations rejects the reported position, even if the position is correct. This probability is given by

$$Pr_{FP}^{n} = 1 - (Pr(-k\sigma < d_F^c - d_F^m < k\sigma))^n \quad (13)$$

The frequency of false negatives is defined as the probability that all the base stations accept the reported position even if this position is false. This probability is given simply as a probability of attacker's success for n covert base stations:

$$Pr_{FN}^{n} = (\frac{4k\sigma}{R})^n \quad (14)$$

Figure 8 shows the the frequency of false positives and false negatives as a function sensitivity s. Here, s is defined as $1/k$. Sensitivity s is thus inversely proportional to the expected error Δ and is a measure of how sensitive is the position verification to errors; if $s = \infty$, this means that the system is very sensitive, and that positioning and ranging errors will are not tolerated, if $s = 0$, this means that the system tolerates any error. Consequently, the frequencies of false positives and false negatives depend on s.

Figure 8 shows the frequencies of false positives and false negatives for 10 and 5 covert base stations, and for $\sigma = 0.005R$ (0.5% of R) and $\sigma = 0.01R$ (1% of R). The emphasis in these figures is on the crossover error rate. The crossover error rate is the error rate at which the false positive frequency equals the frequency of false negatives. From these figures we observe, as expected, that with the increase in the number of covert base stations, and with the reduction of the standard deviation of the positioning and ranging error σ, the crossover error rate can significantly reduced. If the number of covert base stations is 5 and if $\sigma = 0.01$, the crossover error rate will be 0.0002. This error rate is significantly reduced to 2×10^{-9} if the σ is reduced to 0.005 and if the number of covert base stations is increased to 10.

Even if the crossover error rate is a good indicator of system performance, we emphasize that the security of the system can be significantly improved if the system can allow for a higher false positive frequency. We show on Figure 9 the frequency of false negatives (probability of attacker's success) as a function of the number of covert base stations, given that the frequency of false negatives is set to 1%. This figure shows that with the frequency of false negatives set to 1%, the probability of attacker's success is significantly lower than the crossover error rate. We therefore observe that with 5 or more covert base stations, the probability of attacker's success is lower than 10^{-5} with standard deviation of error smaller than $0.03R$.

We can also observe that with positioning systems that exhibit high standard deviation of error (up to 30% or the region radius R), the probability of attacker's success can still be significantly reduced by increasing the number of covert base stations. For example, with $\sigma = 0.2R$ and 20 hidden stations, the probability of attacker's success is only 2×10^{-6}.

E. Integration with existing positioning systems

A number of systems for positioning and ranging of wireless devices have already been proposed, based on the propagation of RF, ultrasound and infrared signals. Most of these systems can be adapted to work with covert base stations. Here, we present a short overview of the precision and area sizes of existing positioning and ranging systems and we discuss how they can be integrated with secure positioning based on covert base.

If positioning is based on GPS, the accuracy of the positioning will be in 95% of cases better than $1m$. RF time of flight techniques being developed for positioning GSM and CDMA Position aim to provide accuracy of 50-100m and 10m, in the case of UL-TOA, GSM and AGPS, CDMA, respectively. Note here that these systems are designed for area and cell sizes which can have radiuses of 500m (in highly dense urban areas) to 35km (in countryside). Indoor, positioning with WiFi based on signal strength measurements with location fingerprinting can achieve positioning accuracy of 2-3m, whereas ultrasound-based ranging and positioning systems can be accurate up to several centimeters. Ultra wide band (UWB) time-of-flight based systems work both indoor and outdoor. Indoor they can achieve ranging precision better than 1m for ranges of up to 50m and positioning accuracy of up to 15cm. Outdoor the accuracy of UWB positioning and ranging systems can be also very high, approx. 1m for distances of up to 2km [16]. All the numbers presented in this paragraph are rough approximations of accuracies of these systems; each of these systems can perform better or worse, if one or more of system parameters change.

Here, we use the term accuracy very loosely as the measures of accuracy vary from one system to another. For example, if GPS positioning is used for providing position reference to a device, and UWB ranging is used for position verification, the standard deviation of the error can be estimated at up to 4 meters. Given that

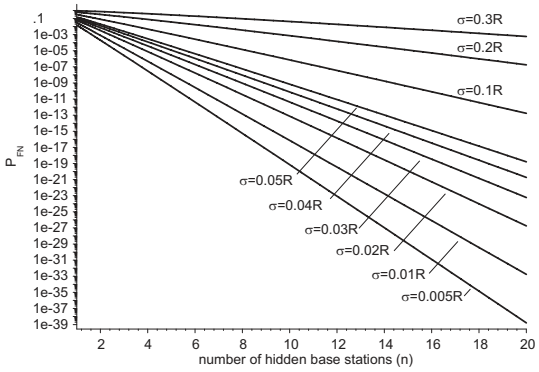

Fig. 9. The frequency of false negatives (probability of attacker's success) if the frequency of false positives is set to $0.01R$.

the range of UWB positioning can be up to 2km than $\sigma < 0.005R$. Indoor, if ultrasound is used for positioning and ultrasonic ranging for verification, we can assume the standard deviation of error to be of the order of 20 centimeters and ranges up to 20m, meaning that $\sigma = 0.01R$. As we have shown in Figures 8 and 9, the probability of attacker's success in these scenarios will can then be as low as 10^{-35} (in best case).

VII. Related work

In the last decade, a number of indoor positioning systems were proposed, based notably on infrared [43], ultrasound [44], [35], received radio signal strength [3], [20], [7] and time-of-flight radio signal propagation techniques [27], [15]. These positioning techniques were then extended and used for positioning in sensor and ad hoc networks [13], [6], [9], [33], [32], [42], [30], [14].

Recently, a number of secure distance and location verification have been proposed. Brands and Chaum [5] proposed a distance bounding protocol that can be used to verify the proximity of two devices connected by a wired link. Sastry, Shankar and Wagner [41] proposed a new distance bounding protocol, based on ultrasound and radio wireless communication. In that work, the authors also propose to make use of multiple base stations to narrow down the area in which the nodes lie. However, as this proposal is based on ultrasound distance bounding, it can therefore be used only for the verification of nodes' positions, and only if external nodes have no access to the area of interest. In [22], the authors propose a mechanism called "packet leashes" that aims at preventing wormhole attacks by making use of the geographic location of the nodes (geographic leashes), or of the transmission time of the packet between the nodes (temporal leashes). Kuhn [25] proposed an asymmetric security mechanism for navigation signals. That proposal aims at securing systems like GPS [18]. Capkun and Hubaux [10] propose a technique called verifiable multilateration, based on distance-bounding, which enables a local infrastructure to verify positions of the nodes. They further show how that technique can be extended for secure positioning of a network of sensors. Lazos et al. [26] proposed a set of techniques for secure positioning of a network of sensors based on directional antennas and distance bounding. Li et al. [28] propose statistical methods for securing localization in wireless sensor networks. Liu et al. [29] propose techniques for the detection of malicious attacks against beacon-based location discovery in sensor networks, based on consistency of received beacons.

Recently, a number of proposals have been made to protect the anonymity and location privacy of wireless devices [36], [19], [37], [40], [23], [24].

VIII. Conclusion

In this work, we proposed a novel approach to secure positioning based on covert (hidden and mobile) base stations. This approach enables secure positioning with a broad spectrum of positioning techniques: ultrasonic or RF, based on received signal strength or on time of signal flight. We have demonstrated that that this approach can be easily integrated with several existing node-centric and infrastructure-centric positioning schemes. We have shown how security of this approach depends on the precision of the positioning systems and on the number of covert base stations.

Our future work includes implementations of our schemes and their evaluation in various indoor and outdoor scenarios. We furthermore intend to investigate the applicability of position verification to secure positioning in mobile ad hoc networks. We also intend to investigate in more detail the privacy implications of our approach.

References

[1] Amigobot. http://www.amigobot.com/.

[2] C. Avin and C. Brito. Efficient and Robust Query Processing in Dynamic Environments Using Random Walk Techniques. In *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2004.

[3] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *Proceedings of InfoCom*, 2000.

[4] S. Bergbreiter and K. S. J. Pister. CotsBots: An Off-the-Shelf Platform for Distributed Robotics. In *Proceedings of IROS*, 2003.

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

[6] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low cost outdoor localization for very small devices. *IEEE Personal Communications Magazine*, 7(5):28–34, October 2000.

[7] P. Castro, P. Chiu, T. Kremenek, and R. Muntz. A Probabilistic Room Location Service for Wireless Networked Environments. In *Proceedings of the Third International Conference Atlanta Ubiquitous Computing (Ubicomp)*, volume 2201. Springer-Verlag Heidelberg, September 2001.

[8] Haowen Chan, Mark Luk, and Adrian Perrig. Using Clustering Information for Sensor Network Localization. In *Proceedings of IEEE Conference on Distributed Computing in Sensor Systems (DCOSS 2005)*, June 2005.

[9] S. Čapkun, M. Hamdi, and J.-P. Hubaux. GPS-free Positioning in Mobile Ad-Hoc Networks. *Cluster Computing*, April 2002.

[10] S. Čapkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of InfoCom*, 2005.

[11] S. Čapkun, J.-P. Hubaux, and L. Buttyán. Mobility Helps Peer-to-Peer Security. *IEEE Transactions on Mobile Computing*, to appear 2005.

[12] K. Dantu, M. H. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. Sukhatme. Robomote: Enabling mobility in sensor networks. In *Proceedings of the International Conference on Information Processing in Sensor Networks*, 2005.

[13] L. Doherty, K. Pister, and L. El Ghaoui. Convex position estimation in wireless sensor networks. In *Proceedings of InfoCom*, April 2001.

[14] T. Eren, D. Goldenberg, W. Whiteley, Y.R. Yang, A.S. Morse, B.D.O. Anderson, and P.N. Belhumeur. Rigidity, computation, and randomization in network localization. In *Proceedings of InfoCom*, 2004.

[15] R.J. Fontana. Experimental Results from an Ultra Wideband Precision Geolocation System. *Ultra-Wideband, Short-Pulse Electromagnetics*, May 2000.

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

[17] J. Friedman, D. Lee, I. Tsigkogiannis, S. Wang, D. Chao, D. Levin, M. Srivastava, and W. Kaiser. Ragobot: A New Hardware Platform for Research in Wireless Mobile Sensor Networks. In *Proceedings of International Conference on Distributed Computing in Sensor Systems*, 2005.

[18] I. Getting. The Global Positioning System. *IEEE Spectrum*, December 1993.

[19] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. In *Proceedings of WMASH*, 2003.

[20] J. Hightower, G. Boriello, and R. Want. SpotON: An indoor 3D Location Sensing Technology Based on RF Signal Strength. Technical Report 2000-02-02, University of Washington, 2000.

[21] L. Hu and D. Evans. Localization for mobile sensor networks. In *Proceedings of MobiCom*, 2004.

[22] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *Proceedings of InfoCom*, 2003.

[23] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing Wireless Location Privacy Using Silent Period. In *Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC)*, 2005.

[24] J. Kong and X. Hong. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks. In *Proceedings of MobiHoc*, 2003.

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

[26] L. Lazos, S. Čapkun, and R. Poovendran. ROPE: Robust Position Estimation in Wireless Sensor Networks. In *Proceedings of IPSN*, 2005.

[27] J.-Y. Lee and R.A. Scholtz. Ranging in a Dense Multipath Environment Using an UWB Radio Link. *IEEE Journal on Selected Areas in Communications*, 20(9), December 2002.

[28] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks. In *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2005.

[29] D. Liu, P. Ning, and W. Du. Attack-Resistant Location Estimation in Sensor Networks. In *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2005.

[30] D. Moore, J. Leonard, D. Rus, and S. Teller. Robust distributed network localization with noisy range measurements. In *Proceedings of the ACM Conference on Networked Sensor Systems (SenSys)*, pages 50–61. ACM Press, 2004.

[31] L. Navarro-Serment, R. Grabowski, C. Paredis, and P.K. Khosla. Modularity in Small Distributed Robots. In *Proceedings of the SPIE conference on Sensor Fusion and Decentralized Control in Robotic Systems II*, 1999.

[32] D. Niculescu and B. Nath. Ad hoc positioning system (aps) using aoa. In *Proceedings of InfoCom*, 2003.

[33] D. Niculescu and B. Nath. DV Based Positioning in Ad hoc Networks. *Journal of Telecommunication Systems*, 22(4):267–280, 2003.

[34] V. Van Nostrand. *Mathematics of Statistics*. Princeton, NJ, 1962.

[35] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The Cricket location-support system. In *Proceedings of MobiCom*, 2000.

[36] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *Pervasive Computing*, January-March 2003.

[37] I. W. Jackson. Anonymous Addresses and Confidentiality of Location. In *Proceedings of International Workshop on Information Hiding*, 1996.

[38] M. G. Kendall and P.A.P. Moran. *Geometrical Probability*. Hafner, New York, 1963.

[39] R. C. Shah, S. Roy, S. Jain, and W. Brunette. Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks. In *Proceedings of the IEEE Workshop on Sensor Network Protocols and Applications (SNPA)*, May 2003.

[40] Y.-C. Hu and H. J. Wang. Location Privacy in Wireless Networks. In *Proceedings of the ACM SIGCOMM Asia Workshop*, 2005.

[41] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location claims. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 1–10. ACM Press, September 2003.

[42] A. Savvides, C.-C. Han, and M. B. Strivastava. Dynamic fine-grained localization in Ad-Hoc networks of sensors. In *Proceedings of MobiCom*, 2001.

[43] R. Want, A. Hopper, V. Falcao, and J. Gibbons. The Active Badge Location system. *ACM Transactions on Information Systems*, 10(1):91–102, 1992.

[44] A. Ward, A. Jones, and A. Hopper. A New Location Technique for the Active Office. *IEEE Personal Communications*, 4(5), October 1997.