

# Secure Location Verification With Hidden and Mobile Base Stations

Srdjan Čapkun\* Kasper Bonne Rasmussen\* Mario Čagalj† Mani Srivastava‡

\*Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland, {capkuns,kasperr}@inf.ethz.ch

†Department of Electronics, FESB, University of Split, 21000 Split, Croatia, mario.cagalj@fesb.hr

‡Electrical engineering Department, University of California, Los Angeles, CA, 90095, mbs@ucla.edu

**Abstract**—In this work, we propose and analyse a new approach for securing localization and location verification in wireless networks 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 mobile ad-hoc and sensor networks.

## I. INTRODUCTION

In the last decade, researchers have proposed a number of localization and ranging techniques for wireless networks [50], [51], [35], [4], [20], [10]. 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 localization 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 locations of honest nodes. Localization 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. Localization systems based on ultrasound time of flight (US ToF) and those based on measurements of signal strength of radio signals (RF RSS) are particularly 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 localization techniques were proposed [25], [26], [48], [28], [29] to cope with these problems. These mechanisms rely on GPS, high speed hardware, directional antennas, robust statistics or spread spectrum techniques using spreading codes. An efficient implementation of these protocols remains a challenge, however, since almost all of them rely on ToA ranging and generally assume fast processing hardware (ns) at the prover (except in the case of ultrasound implementations, which are limited in range). Our proposal works with simple ranging (not

with distance-bounding) and therefore does not require fast processing at the prover (claimant). Our proposal works equally well using any kind of ranging, even low-cost RSSI-based methods (e.g., [4], [20], [10])

Our approach to secure localization relies on a set of covert base stations. By covert base stations (CBS), we mean base stations whose locations are not known by the attacker at the time of the execution of the secure localization. In our system, locations 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.

The aim of the protocols in this paper is to ensure that a node can not lie about its position and thus pretend to be in a different physical location than the one it occupies, e.g., a node can not (successfully) claim to be in a room if the node is outside that room (e.g., for location-based access control).

We show through three example protocols how covert base stations can be used to secure node-centric and infrastructure-centric localization, as well as for localization and location-verification in ad-hoc and sensor networks. We discuss how security of the proposed protocols depends on the precision of the localization 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 localization in infrastructure-centric and node-centric systems, respectively. In Sections V and VI, we show how mobile base stations can be applied to secure localization in sensor and mobile ad-hoc networks. In Section VII, we analyze our schemes. In Section VIII, we overview the related work. We conclude the paper in Section IX.

## 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 localization infrastructure. Here, by covert base stations we mean those base stations whose locations are known only to the authority controlling the verification infrastructure. To

prevent their locations from being 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 locations or can obtain their locations securely and passively (e.g., through secure GPS [25]). Here, we assume that the attackers cannot tamper with these locations 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 ultrasonic interface 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. We replace the public and covert base stations with mobile base stations, and we assume that their mutual communication is wireless.

Finally we assume that the nodes (legitimate or otherwise) have a limited number of attempts to prove their location to the infrastructure. This is needed in order to prevent that the nodes simply try different distances until they get it right.

### 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 localization infrastructure that it is at a false position. External attacks are those in which an external attacker convinces an honest node and the localization infrastructure that the node is at a different position from its true position (i.e., the attacker *spoofs* a node's position).

We observe two types of localization systems: node-centric and infrastructure-centric. By a node-centric localization system, we mean that a node computes its position by observing signals received from public base stations with known locations. If the localization system is *node-centric*, internal attacks are generally straightforward; a the attacker simply lies about the position that it computed. *Infrastructure-centric* localization systems are those in which the infrastructure computes locations 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 (e.g., using directional antennas).

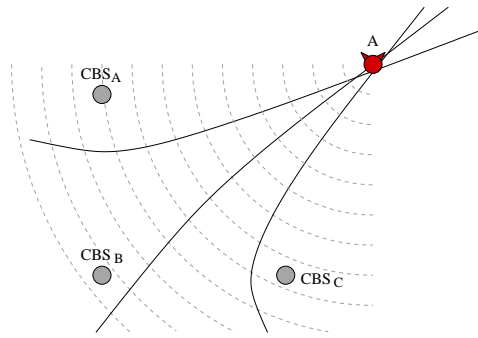


Fig. 1. An example of localization with Time Difference Of Arrival. The base stations  $CBS_A$ ,  $CBS_B$  and  $CBS_C$  measure the differences of signal arrival times, and computes the position of the attacker.

Attacks by external attackers are similar to those performed by internal attackers. An external attacker can perform timing attacks by delaying the signal (through jamming) or speeding it up (through wormhole attacks [22], [45]). The attacker can also perform power level modification attacks by replaying signals at different power levels.

### III. INFRASTRUCTURE-CENTRIC LOCALIZATION WITH HIDDEN BASE STATIONS

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

TDOA is the process of localizing a source of signal in two (respectively three) dimensions by finding the intersection of multiple hyperbola based on the time difference of arrival between the signal reception at multiple base stations. Using two hyperbolas (three base stations) we can obtain two dimensional device locations, and using three hyperboloids (four base stations) we can determine three dimensional locations. 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 localization 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 localization 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 the nodes location with TDOA, and check if this location is consistent with the time differences. By consistent we mean that the computed position is not too far from the hyperbola 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 locations of base stations only with a very low probability. The protocol is executed as shown on Figure 2.

#### Security analysis

Here,  $p$  is a position of node  $A$  computed from the measured time differences and it is the solution to the following

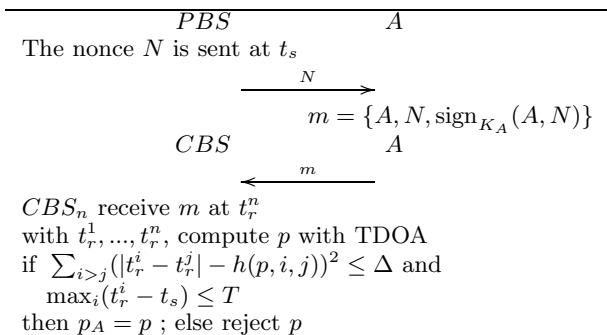


Fig. 2. TDOA with hidden base stations

least-square problem:

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

where  $h(p^*, i, j)$  is the expected difference of signal reception times at  $CBS_i$  and  $CBS_j$  (based on the known signal propagation time), if the signal is sent from position  $p^*$  and  $|t_r^i - t_r^j|$  is the measured difference at  $CBS_i$  and  $CBS_j$ .  $\Delta$  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 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. 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  $\Delta$ . Essentially,  $\Delta$  defines the size of the attacker's guessing space. Simply, if  $\Delta$  is large, a false position will be more likely accepted, as the tolerance to inconsistencies will be higher. In Section VII, we investigate in more detail the relationship between  $\Delta$  and the attacker's success.

In addition, we need to consider one more external attack on TDOA - an external wormhole. This attack is performed as follows: (1) Attacker jams the original localization 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 and have faster processing 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 pre-

vented 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 this simple challenge-response scheme could be replaced by a more efficient distance-bounding protocol [6], [46], in which case, 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. The same attacks can also be prevented through precise time synchronization. However, if the base stations and the devices can perform (expensive) distance-bounding protocols, other (distance-bounding based) approaches, like Verifiable Multilateration [48] can be used for the verification of devices' location claims. The proposed TDOA-based location verification scheme (without distance bounding) is therefore a low-cost alternative for location verification in scenarios in which false location claims do not benefit the attacker, and/or in those scenarios in which the attacker does not have the ability to perform the described wormhole attack (i.e., either cannot jam the communication between the node and the base station or does not have fast-processing hardware).

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 localization signals disclosing its location. Other attacks are possible on node's location privacy [38], [19], [39], [42], [23], [24], but coping with these attacks is out of the scope of this paper.

#### IV. NODE-CENTRIC LOCALIZATION WITH HIDDEN BASE STATIONS

In this section, we present a protocol for secure localization in node-centric localization systems. Here, we assume that the node computed its position through a non-secure localization 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 a covert base station. The 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 ultrasonic ranging).

Our protocol is shown on Figure 3. Here  $N$  is a nonce generated by the public base station,  $\Delta$  is a combined localization 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

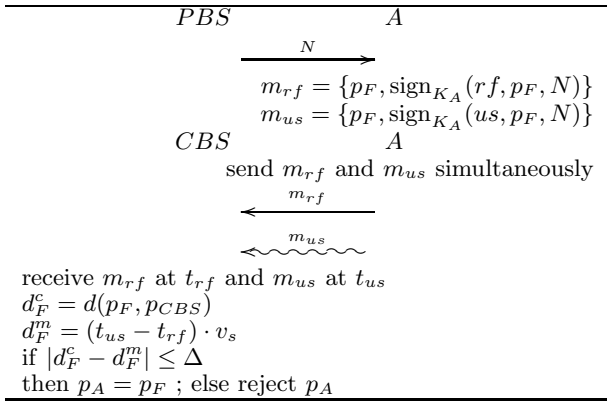


Fig. 3. Position verification with hidden base stations

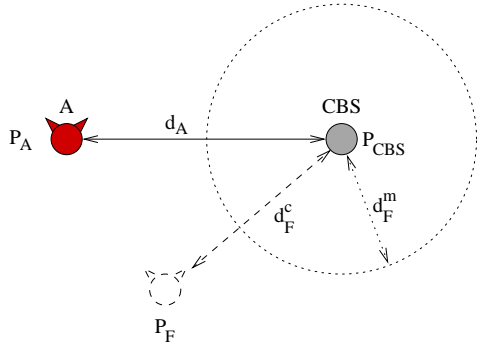


Fig. 4. False position report by node  $A$  to the covert base station.  $p_A$  is the true node position,  $p_F$  is the fake node position (reported by  $A$  to  $CBS$ ),  $p_{CBS}$  is the position of  $CBS$ .  $d_F^c = d(p_F, p_{CBS})$  is the (false) distance between  $CBS$  and  $A$ , computed 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  $p_A = p_F$ .

base station to verify the reported position.  $PBS$  sends a challenge to the node  $A$ , which then replies by sending radio and ultrasonic 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 ultrasonic 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  $A$ . An illustration of a fake position report is shown in Figure 4. 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 localization and ranging error  $\Delta$ , then the position is rejected; else, the position is accepted as true node position. An additional verification is made 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 or with *any* other passive ranging technique available, including passive RF ranging.

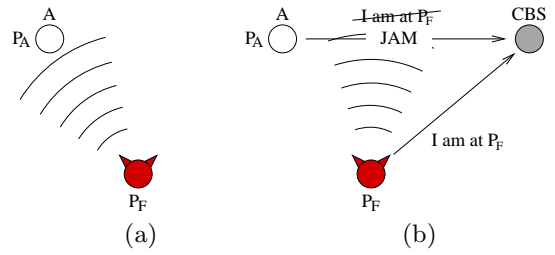


Fig. 5. Position spoofing attack. (a) The attacker spoofs node  $A$  into believing that it is at the attacker's location  $P_F$  (e.g., using a fake GPS station), then the attacker jams the localization message (b) and replays it from its own position there by fooling the  $CBS$  into accepting the position as real (i.e., the distance will match).

### Security analysis

An internal attack in node-centric localization 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 VII.

External attacks against position verification are more complex and include position spoofing, jamming and message replays. Figure 5 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 localization 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 tightly 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 require 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 [6], 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 node's position. This attack 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.

A cloning attack is an attack in which the attacker successfully compromises a node to such a degree, that private keys and other secret node-specific information can be copied.

The attacker can now deploy any number of copies of the original node throughout the network. Our protocols make no attempt to detect cloning attacks, however, fingerprinting [36] could be used as a way of distinguishing the copies from the original. It should be noted that a cloning attack does not constitute a breach of security in, e.g., an access control application, since the attacker still needs to place a clone within the access controlled area.

Finally the attacker can interfere with the communication of legitimate nodes to change the time of flight of a signal, thereby making it seem as if the nodes are reporting false positions. Some applications might want to exclude nodes after a certain number of false positions have been received and in such a case this attack could be very damaging, however, this is entirely application and policy specific. Excluding a node after a number of false positions have been received is straightforward as the protocol requires the node to send signed messages. While an attacker might succeed in performing a denial of service attack and thus introduce more false positives, the attacker can only create a false negative with a very small probability (see section VII).

## V. SECURE LOCALIZATION 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 [41], [49], [21]. Many mobile platforms have emerged as a result: Amigobot [1], Cotsbot [5], Millibot [31], Robomote [12], and Ragobot [17].

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

### A. Scenario

In our scenario we rely on mobile base stations. We show how mobile base stations can be used to secure localization and to verify the locations of sensor nodes.

We assume that the sensors compute their locations through one of the non-secure localization algorithms [13], [7], [47], [33], [32], [44], [30], [14], [11].

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.

### B. 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 localization 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.

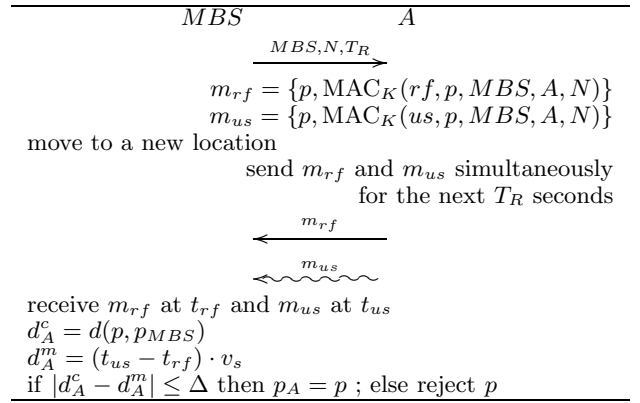


Fig. 6. Position verification with mobile base stations.

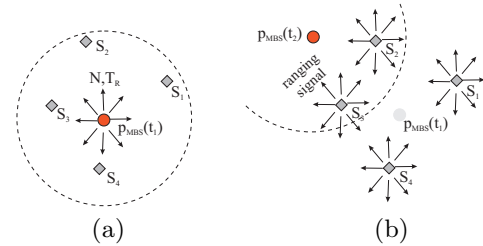


Fig. 7. Position verification in sensor networks. A mobile base station (MBS) verifies locations of nodes; (a) at time  $t_1$  MBS challenges sensor nodes; (b) at time  $t_2 > t_1$  the sensors reply to the challenge and their locations are verified by MBS.

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 shown in Figure 6. Here,  $K$  is the secret key shared between the mobile station  $MBS$  and the sensor  $A$ . After receiving a localization message from the  $MBS$ ,  $A$  is supposed to send a response for the next  $T_R$  seconds. In order to avoid interference from other nodes who also received the same localization message, a suitable MAC protocol must be used to ensure that everyone has access to the channel.  $T_R$  is also the time within which  $MBS$  must move to a new location and receive the response from all the nodes that are still in range.

$T_R$  must not give away any information about the distance from the current transmission position to the next verification position. Further more,  $T_R$  must allow enough time for the  $MBS$  to wait a few seconds at its new location until all the nodes have replied.

The operation of our protocol is illustrated on Figure 7. 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 need 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 locations (this procedure is the same as in the position verification protocol presented in Section IV).

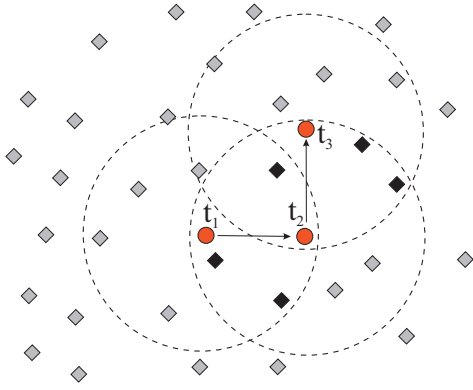


Fig. 8. Progress of position verification in sensor networks with mobile base stations. MBS moves from position  $p_{MBS}(t_1)$  to  $p_{MBS}(t_2)$  and  $p_{MBS}(t_3)$ .

### C. Mobile base station coverage and simulation

Typically, the MBS can perform simultaneous verification of locations of multiple sensors. If, at each motion step  $t_2$ , the MBS moves within the circle defined by its power range, 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 the MBSs power range<sup>1</sup>. This is because the intersection of the MBSs power ranges at  $t_1$  and at  $t_2$  will be at least 39% of the circle surface, given that the MBS moved within its previous power range. At time  $t_1$  the MBS broadcasted a challenge to the nodes, and at time  $t_2$ , the nodes replied. After position verification, the MBS issues another challenge for the nodes in its power range whose locations were not verified; then, the MBS moves again and waits for their reply. Hence, as the MBS moves through the network, it will only verify locations of those sensors which were in the intersections of two subsequent power ranges of the MBS. This is illustrated on Figure 8. The trajectory of the MBS needs to be unpredictable for the sensor nodes, even if the sensors collude. One way to ensure this, is to have the MBSs move according to a 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 [41], [3], the authors provide a set of analytical and simulation results for coverage times of mobile stations on sensor grids.

If the sensors are randomly distributed, the coverage time will depend on the radio range and on the movement range of the MBS (and speed of course). In Figure 9 is a plot of the coverage as a function of the movement range. A single mobile base station moves according to a random walk for 60 seconds in a  $500 \times 500$  meter area with 300 nodes. The four different curves are four different transmission ranges. It is clear from the figure that the best results are achieved if the movement range and the transmission range are equal (or very similar). This is because if the movement range is smaller than the transmission range the MBS does not take full advantage of the size by not moving far enough, and if

<sup>1</sup>This also assumes that either the MBS and the nodes have the same transmission radius or the MBS have a high gain antenna that will enable it to receive the reply from within its own transmission radius.

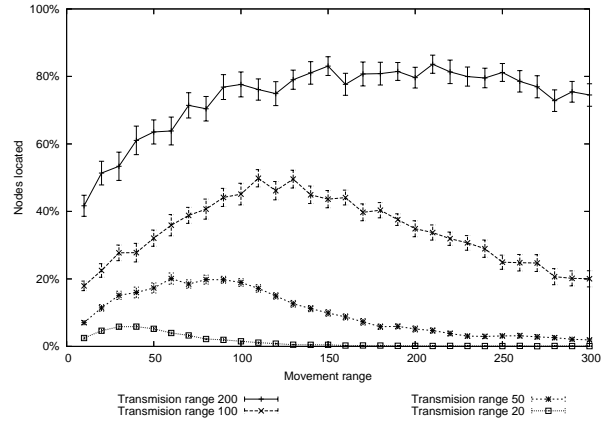


Fig. 9. Mobile base station coverage for different values of transmission and movement range (step size). Every point on the graph is the average result of 50 simulations, the vertical bars indicate the 95% confidence interval.

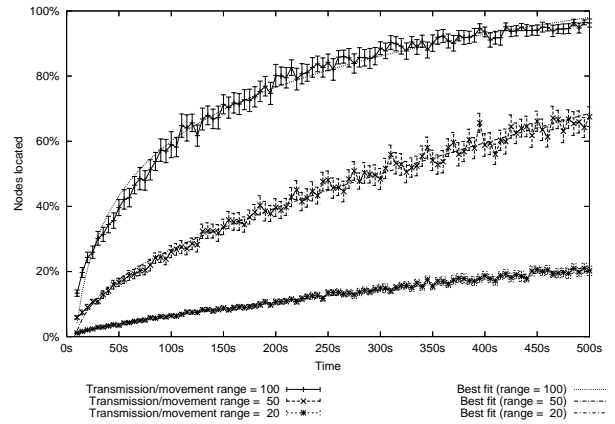


Fig. 10. Mobile base station coverage as a function of time. Every point on the graph is the average result of 50 simulations, the vertical bars indicate the 95% confidence interval.

the movement range is larger than the transmission range the MBS will move too far away to receive the replays from all the nodes. Of course the coverage improves when the transmission/movement range is increased.

Figure 10 shows the coverage time of 300 sensors placed randomly throughout an area of  $500 \times 500$  meters. One node is chosen to be a mobile base station and moves through the network using random walk. At each position the MBS listens for the reply to previous challenges, issues a new challenge, picks a new point on the disc described by its transmission range and moves there. The speed at which the MBS moves is set to  $50m/s$ , about the speed of a small drone over a battlefield, and the node timeout  $T_R$  is set to 5 seconds.

As expected the performance increases with the transmission/movement range as more nodes are localized in each step. A function on the form

$$C = at + b \ln(t) + c \quad (1)$$

can be fitted to each of the three data plots, where  $C$  is the relative coverage and  $t$  is the time. The parameters  $a$ ,  $b$  and  $c$  are determined by the size of the area, the speed of the MBS and the transmission/movement range.

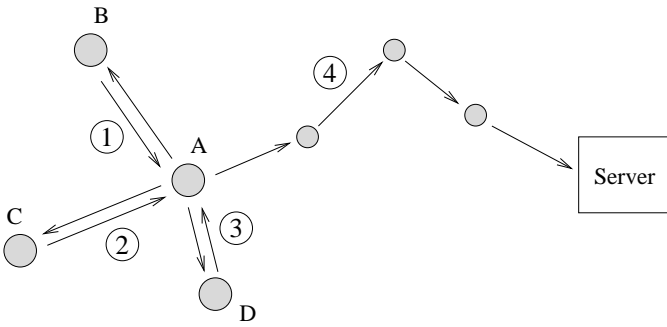


Fig. 11. Node  $A$  gathers signed witness statements about its location in order to update a central location database (residing on the server  $S$ ). Each using the protocol in Figure 12, nodes  $B$ ,  $C$  and  $D$  first verify the location of  $A$  (steps 1,2,3) and then send (to  $A$ ) signed statements about its location.  $A$  then sends its position along with collected witness statements (positive and negative) in a confidential message to the server (step 4).

Using (1) it is possible to estimate the required equipment specifications (i.e., speed and transmission range) needed to cover a particular area in a particular amount of time.

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.

## VI. LOCATION VERIFICATION IN MOBILE AD-HOC NETWORKS

In this section, we show how our node-centric position verification protocols (Section IV) can be used for location verification and secure location updates in mobile ad-hoc networks. The scenario presented in this section differs from the scenario in Section V in that there are no dedicated mobile base stations that move around and localize nodes. Instead, in this scenario, nodes obtain their positions using a global positioning system (e.g., GPS [18]), and rely on their neighbors for position verification. We further assume that all nodes in the network have passive ranging capabilities; we describe our protocols assuming that the nodes implement US-based passive ranging, although other passive ranging scheme can be used (e.g., RSSI-based ranging).

### A. Location database update

We consider a scenario in which, a node  $A$  wants to update its location in a central location database. This update can be motivated by a need to prove that the node was at a specific location at a specific time (e.g., to support secure location-based routing). In order to update its location, the node will rely on the (signed) statements of its neighbors. In order to ensure the authenticity of these statements, we assume that all nodes have a public/private key pair and that each node shares a secret key with the location database server. This scenario is illustrated in Figure 11.

In order to update its location at the server, node  $A$  executes the protocol shown in Figure 12.  $A$  starts the protocol by announcing on both RF and US channels its location in a broadcast signed message containing its location  $P_A$ , and the timestamp  $T_A$ .  $A$ 's neighbors (e.g.  $B$ ) verify  $A$ 's location claim and then issue timestamped and signed statements  $stat_B$  regarding  $A$ 's claim. These statements can be either

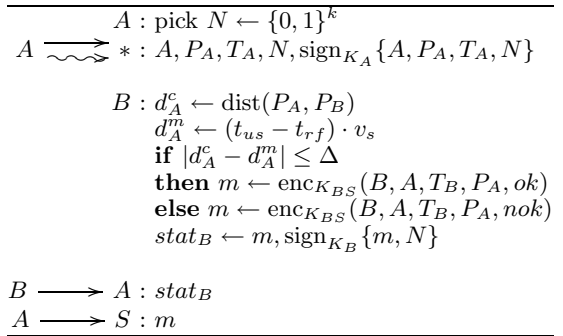


Fig. 12. Node  $B$  issues a witness location statement, attesting if  $A$  was at location  $P_A$  at time  $T_B$ . Note that  $A$  does not know if  $B$ 's witness statement is positive ( $ok$ ) or negative ( $nok$ ).  $A$  forwards this statement to the server  $S$  (in a private message) (possibly over multiple hops).  $A$ 's location  $P_A$  is therefore disclosed only to its surrounding nodes (for location verification) and to the location server  $S$ , and is not disclosed to other network nodes.

positive (containing the string ' $ok$ ') or negative (containing the string ' $nok$ '), stating that the reported location  $P_A$  is correct or incorrect, respectively; here  $K_{BS}$  is the secret key shared between  $B$  and the server  $S$ . Note that  $A$  does not know if  $B$ 's witness statement is positive or negative. Upon verifying that the statement originated from  $B$ ,  $A$  forwards this confidential message to the server  $S$  (possibly over multiple hops); alternatively,  $B$  can directly report its statement to the server.  $A$ 's location  $P_A$  is therefore disclosed only to the location server  $S$  and to its surrounding nodes (for location verification purposes). The location server collects statements about node locations, and infers if nodes' claimed locations, and location statements of their neighbors match. The information collected at the server can then be used by the network nodes e.g., for secure location-based routing, and by the server e.g., for the detection of malicious or selfish node behavior. We note that before each location verification a node ( $B$ ) needs to estimate if its position is sufficiently unpredictable for the prover ( $A$ ). This,  $B$  can do locally by monitoring how much it moved since its last transmission.

### B. Security analysis

An attacker that wants to falsify its location must make the distance calculated at the receiver, match the position the attacker reports. We analyze this in detail in Section VII. However, one point is of special significance in the case of mobile ad-hoc networks; since nodes mutually verify each-others' locations, they will equally, by transmissions or by explicit disclosure (for verification purposes), disclose their locations. If an attacker, therefore, listens to the communication between the claimant node and its witnesses, it will at least observe the location of the claimant and at most the locations of its verifiers. If the attacker then initiates the verification of its own location right after, it can successfully cheat on its location, since it knows the locations of all its neighbors. To prevent such attacks, nodes monitor how much they moved since their last transmission, or how much time elapsed since their last transmission. Only if they moved significantly and/or enough time has passed since their last transmission, will the nodes engage in a location verification protocol as witnesses. As we discuss

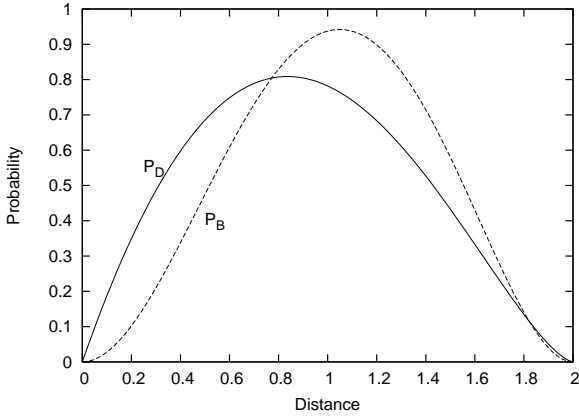


Fig. 13. Probability distribution function of the distance  $d_F^c = d(p_F, p_{CBS})$  on a disk ( $P_D$ ) and in a ball ( $P_B$ ), when  $p_{CBS}$  and  $p_F$  are chosen uniformly over the disk and ball, respectively.

above, the proposed protocol preserves nodes' privacy from all nodes except from their neighbors (that need to know the node's location in order to verify it).

## VII. ANALYSIS

In this section, we analyze the likelihood that an (internal) attacker succeeds in cheating our secure position verification schemes by guessing the locations of or the distances to 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 localization system.

First, we focus on the position verification protocol described in Section IV. We define the attacker's success as the event where 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 be realized only if  $|d_F^c - d_F^m| \leq \Delta$ . This essentially means that an attacker needs to guess the distance to the covert base station  $d_A$ , in order to engineer the signals such that the CBS measures a  $d_F^m$  equal to the distance to the reported (fake) position  $d_F^c$ . The probability of attackers success is therefore

$$P(|d_F^c - d_F^m| \leq \Delta \mid p_F \neq p_A) \quad (2)$$

In our analysis we assume that the localization 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 and the hidden base station are placed uniformly on a disk/ball. In this case, the probability distribution function (pdf) of the distance between the attacker and the hidden base station is given by [40]:

$$P_D(d_A = d) = \frac{4d}{\pi R^2} \cos^{-1}\left(\frac{d}{2R}\right) - \frac{2d^2}{\pi R^3} \sqrt{1 - \frac{d^2}{4R^2}} \quad (3)$$

for a disk and by

$$P_B(d_A = d) = \frac{3d^2}{R^3} - \frac{9d^3}{4R^4} + \frac{3d^5}{16R^6} \quad (4)$$

for a ball, where  $R$  is the radius of the disk/ball.  $P_D$  and  $P_B$  are shown on Figure 13. The maximum values of these functions are  $P_D(d_A = 0.84R) = 0.809$  and  $P_B(d_A = 1.05R) = 0.942$ . This means that when the attacker is trying to guess the distance to the CBS  $d(p_A, p_{CBS})$ , he will have the highest chance of success if his guess is  $d_A = 0.84R$  (for a disk). In this case, the probability of attacker's success will be:

$$P_{D,uni} = \int_{0.84R-\Delta}^{0.84R+\Delta} P_D dd \approx 0.809 \cdot 2 \frac{\Delta}{R} \quad (5)$$

$$P_{B,uni} = \int_{1.05R-\Delta}^{1.05R+\Delta} P_B dd \approx 0.942 \cdot 2 \frac{\Delta}{R} \quad (6)$$

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

The probability of the 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

$$P_{D,uni}^n \approx \left(0.809 \cdot 2 \frac{\Delta}{R}\right)^n \quad (7)$$

$$P_{B,uni}^n \approx \left(0.942 \cdot 2 \frac{\Delta}{R}\right)^n \quad (8)$$

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

### B. Attacker's maximum success probability

So far, we have assumed that the attackers position  $p_A$  is chosen uniformly, meaning that we have assumed that the position at which the attacker is placed, can be anywhere within the disk/ball. Here, we observe for which position  $p_A$  the attacker will have the highest probability of success. We show that the attacker has the highest probability of success ( $P_{max}$ ) if it chooses its position  $p_A$  at the center of the disk/ball and if it chooses  $d_F^m = R - \Delta$  as its fake measured distance to CBS. This probability is as follows

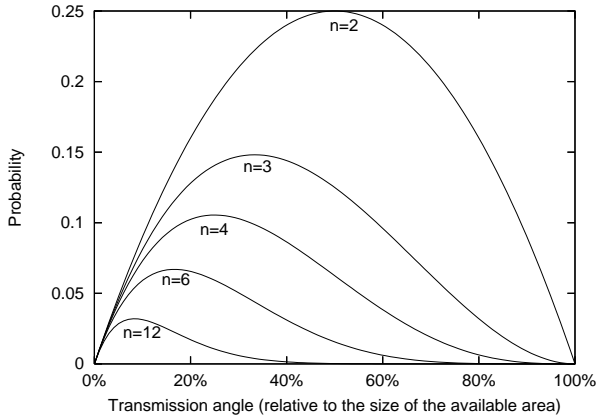


Fig. 14. The probability of successfully guessing the direction of one of the CBS while at the same time not hitting any of the other base stations ( $P_{hit} \cdot P_{mtr}$ ). Note that the angle is relative to the size of the guessing space.

(for a disk):

$$\begin{aligned}
 P_D(d_A \leq d) &= \frac{\pi d^2}{\pi R^2} \\
 P_D(d_A = d \pm \Delta) &= \frac{\pi(d + \Delta)^2 - \pi(d - \Delta)^2}{\pi R^2} \\
 &= \frac{4d\Delta}{R^2} \\
 P_{max_D} &= P_D(d_A = (R - \Delta) \pm \Delta) \\
 &= \frac{4\Delta(R - \Delta)}{R^2} \quad (9)
 \end{aligned}$$

Similarly for the ball, we obtain that  $P_B(d_A = (R - \Delta) \pm \Delta) = \frac{6\Delta(R - \Delta)^2 + 2\Delta^3}{R^3}$ . From this it follows that the maximum probability of the attacker's success given  $n$  CBS is

$$P_{max_D}^n = \left( \frac{4\Delta(R - \Delta)}{R^2} \right)^n \quad (10)$$

$$P_{max_B}^n = \left( \frac{6\Delta(R - \Delta)^2 + 2\Delta^3}{R^3} \right)^n \quad (11)$$

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. Extending the analysis to TDOA

In the case of position verification using TDOA as described in section III there is one additional element that the attacker must consider. If the attacker is to fake his position in a TDOA environment he must also guess the direction in which he needs to point his directional antenna in order to send the delayed message to the correct base station. We will look at the scenario in which the attacker has the highest probability of success which is its case when the attacker positions himself in the center of the verification circle.

If the covert base stations are randomly distributed across the verification space, the probability of the attacker hitting

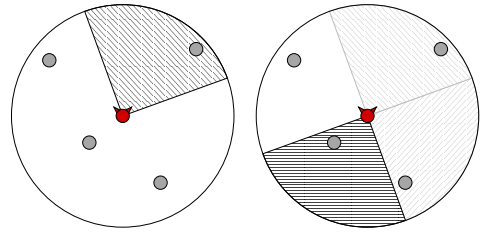


Fig. 15. An example of an attacker guessing the directions to 4 covert base stations in such a way that a transmission to any of the covert base stations would not be received by anyone else.

the correct CBS depends on the angle of his transmission cone. If the angle  $\theta$  is  $0^\circ$  the probability of hitting the correct base station is also 0. If the angle is  $\theta_{max}$  (i.e.,  $360^\circ$  in a full circle) then the probability of hitting the correct CBS is 1. We can write the following relation between probability and angle:

$$P_{hit} = \frac{\theta}{\theta_{max}} = \theta_{rel} \quad (12)$$

where  $\theta$  is the absolute angle and  $\theta_{rel}$  is the relative angle of the transmission cone (relative to the angle of the available space).

Choosing a large transmission angle in order to increase the probability of hitting the correct CBS has one undesired consequence, it also increases the probability that the attacker hits one of the other covert base stations. In order to succeed in his attack, the attacker must hit the correct base station and *not* hit any of the remaining base stations.

The probability of *not* hitting other base stations is given by:

$$P_{mtr} = (1 - \theta_{rel})^{n-1} \quad (13)$$

where  $n$  is the number of base stations (i.e., minimum three in 2D).

The best choice for the attacker is to pick the angle that maximizes his chance to hit the desired CBS but at the same time minimizes the risk of hitting anyone else i.e., the maximum of  $P_{hit} \cdot P_{mtr}$ . It is straightforward to show that the maximum of  $P_{hit} \cdot P_{mtr}$  is  $\frac{1}{n}$ .

In Figure 14  $P_{hit} \cdot P_{mtr}$  is plotted as a function of the relative angle of the transmission cone for  $n = \{2, 3, 4, 6, 12\}$  base stations. If there are four CBS we can see from Figure 14 that the attacker would pick a transmission cone width of one fourth of the guessing space, or  $\theta = 90^\circ$ , giving a probability of successfully guessing the direction of one of the CBS while at the same time not hitting anyone else of 10.5%. But that is only the direction to *one* of the CBSs. Now the attacker must find the next CBS, however, his guessing space is reduced from  $360^\circ$  to  $360^\circ - 90^\circ = 270^\circ$  and the number of base stations is reduced from 4 to 3. Because there are now only three base stations the attacker will choose an angle of one third of the remaining guessing space, or  $90^\circ$ , this gives a probability of successfully guessing the direction of another of the CBS while at the same time not hitting any of the other stations of 14.8%. Now the guessing space is further reduced to  $270^\circ - 90^\circ = 180^\circ$  and the number of base stations is 2. Choosing  $\theta = 90^\circ$  (half the guessing space) the probability is 25%. After this there is only one CBS left and

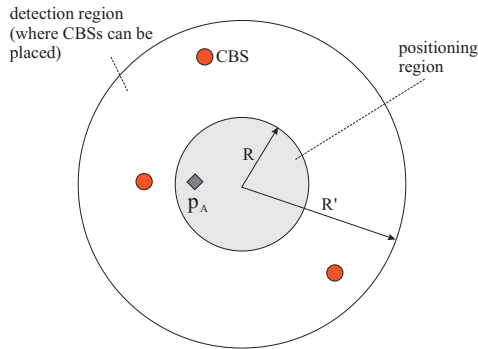


Fig. 16. localization and detection region. If the base stations can be positioned outside of the localization zone, that the probability of the attacker's success can be further decreased.

we know that it is in the last quarter of the original guessing space. The combined probability of correctly aiming four directional antennas at four covert base stations without accidentally hitting any wrong CBS is therefore

$$0.105 \cdot 0.148 \cdot 0.25 = 0.0039$$

Following the above procedure it is easy to see that the combined probability of correctly aiming  $N$  directional antennas at  $N$  covert base stations without accidentally hitting any wrong CBS can be written as

$$\prod_{n=1}^N \frac{1}{n} \left(1 - \frac{1}{n}\right)^{n-1} \quad (14)$$

Where  $N$  is the number of covert base stations in the verification space.

It should be clarified that this probability only covers the aiming of the antennas. If an attacker actually want to cheat on a location in a TDOA environment he must also fake the distance to each of the covert base stations. In the case of four CBSs ( $N = 4$ ) and an acceptable error of  $\Delta = 0.01R$  the maximum probability of successfully falsifying a position is

$$\begin{aligned} P_{success} &= \prod_{n=1}^4 \frac{1}{n} \left(1 - \frac{1}{n}\right)^{n-1} \cdot \left(\frac{4\Delta(R-\Delta)}{R^2}\right)^4 \\ &= 3.9 \times 10^{-3} \cdot 2.5 \times 10^{-6} \\ &= 9.6 \times 10^{-9} \end{aligned}$$

#### D. Further reducing the probability of attacker's success

The 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 (localization region) is the same as the region within which the covert base stations are positioned. However, the covert base stations can also be placed outside of the localization region (around the localization region). The maximal distance from the covert base stations to the localization region will depend on the power range of the attacker's device and on the receiver sensitivity of the base stations. This is illustrated on Figure 16. In this case, the maximum probability of attacker's success is further reduced from  $Pmax_D = \frac{4\Delta(R-\Delta)}{R^2}$

and  $Pmax_B = \frac{6\Delta(R-\Delta)^2 + 2\Delta^3}{R^3}$  to  $Pmax'_D = \frac{4\Delta(R'-\Delta)}{R'^2}$  and  $Pmax'_B = \frac{6\Delta(R'-\Delta)^2 + 2\Delta^3}{R'^3}$ , respectively, as  $R' > R$ .

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

It should be noted for completeness that a sophisticated attacker might try to obtain information about the location of a mobile or covert base station, using a radar based system capable of detecting antenna backscatter (i.e., the energy that is re-radiated by a receiving antenna). However, this energy is very weak compared to the original signal, and the radar signature it generates is no bigger than the signatures from other small metal objects in the environment [8]. For this reason, it would be difficult, if not impossible, for the attacker to detect the presence and/or location of covert/mobile nodes in most (e.g., urban) environments.

#### E. Sensitivity

In this section, we analyze the frequency of false positives and false negatives as a function of the expected localization and ranging error  $\Delta$ . If the authority sets  $\Delta$  to 0, the probability of the attacker's success will be 0, but due to the localization and ranging errors the system will reject all reported locations, even if the device is not faking its position. In this case, the frequency of false positives will therefore be 1. Similarly, if  $\Delta$  is set to  $\frac{1}{2}R$  ( $R$  being the radius of the verification space), then the probability of the attacker's success will be 1 (the attacker will assume that the CBS is  $\frac{1}{2}R$  away and  $\frac{1}{2}R \pm \Delta$  will then cover the entire space). In that case the false locations of the attacker will be accepted every time and the frequency of false negatives will be 1. It is therefore important to set  $\Delta$  such that it minimizes the false negatives and false positives. This means that  $\Delta$  should be chosen as a minimum value that properly reflects localization and ranging errors.

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 localization 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 localization 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  $\Delta$  in terms of  $\sigma$  as follows:

$$\Delta = k\sigma \quad (15)$$

where  $k$  is a positive real number and  $\sigma$  is the standard deviation of  $error$  ( $\sigma = \sqrt{\sigma_P^2 + \sigma_R^2}$  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

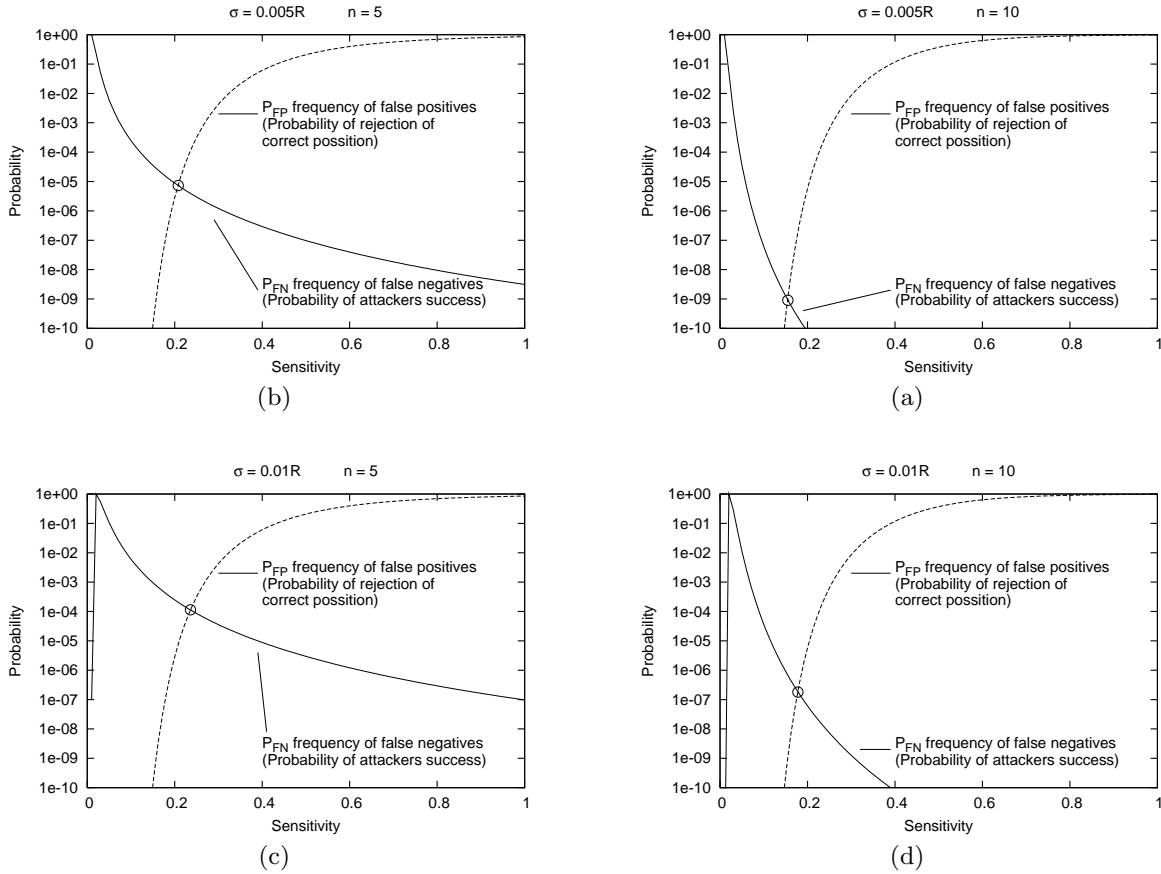


Fig. 17. The frequency of false positives and false negatives, and a crossover error rate for  $\sigma = 0.005R, n = 5$  (a),  $\sigma = 0.005R, n = 10$  (b),  $\sigma = 0.01R, n = 5$  (c),  $\sigma = 0.01R, n = 10$  (d).  $s = 1/k$  is the sensitivity.  $\Delta = k\sigma$  is the tolerated localization and ranging error.  $\sigma$  is the standard deviation of the localization and ranging error. Note that the probability axis is logarithmic.

by [34]:

$$P(-k\sigma < d_F^c - d_F^m < k\sigma) = \frac{2}{\sqrt{\pi}} \int_0^{\frac{k}{\sqrt{2}}} e^{-u^2} du = \text{erf}\left(\frac{k}{\sqrt{2}}\right) \quad (16)$$

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

$$P_{FP} = 1 - P(-k\sigma < d_F^c - d_F^m < k\sigma) \quad (17)$$

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 the attacker's success given by (in 2D):

$$P_{FN} = \frac{4\Delta(R - \Delta)}{R^2} = \frac{4k\sigma(R - k\sigma)}{R^2} \quad (18)$$

For  $n$  covert base stations, these probabilities are defined as follows. The frequency of false positives is defined as the 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

$$P_{FP}^n = 1 - P(-k\sigma < d_F^c - d_F^m < k\sigma)^n \quad (19)$$

Similarly the frequency of false negatives for  $n$  covert base stations 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:

$$P_{FN}^n = \left(\frac{4k\sigma(R - k\sigma)}{R^2}\right)^n \quad (20)$$

Figure 17 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  $\Delta$  and is a measure of how sensitive the position verification is to errors; if  $s = \infty$ , this means that the system is very sensitive, and that localization 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 17 shows the frequencies of false positives and false negatives for 5 and 10 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 localization and ranging error  $\sigma$ , the crossover error rate can significantly reduced. If the number of covert base stations is  $n = 5$  and if  $\sigma = 0.01R$ , the crossover error rate will be about  $1 \times 10^{-4}$ .

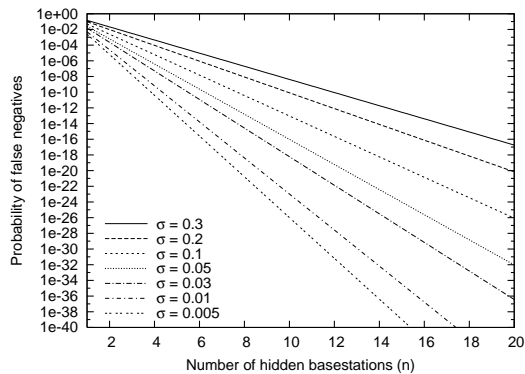


Fig. 18. The frequency of false negatives (probability of attacker success) if the frequency of false positives is set to 1%.

This error rate is significantly reduced to approximately  $1 \times 10^{-9}$  if the  $\sigma$  is reduced to  $0.005R$  and if the number of covert base stations is increased to  $n = 10$ .

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 in Figure 18 the probability of false negatives (probability of attacker’s success) as a function of the number of covert base stations, given that the frequency of false positives is set to 1%. This figure shows that with the frequency of false positives 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 localization 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  $2 \times 10^{-6}$ .

#### F. Integration with existing localization systems

A number of systems for localization 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 localization and ranging systems and we discuss how they can be integrated with secure localization based on covert base stations.

If localization is based on GPS, the accuracy of the localization will be in 95% of cases better than 1m. RF time of flight techniques being developed for localization 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 the countryside). Indoor, localization with WiFi based on signal strength measurements with location fingerprinting can achieve localization accuracy of 2-3m, whereas ultrasound-based ranging

and localization systems can be accurate down to a few centimeters. Ultra wide band (UWB) time-of-flight based systems work both indoor and outdoor [2]. Indoor they can achieve ranging precision better than 1m for ranges of up to 50m and localization accuracy of up to 15cm. Outdoor the accuracy of UWB localization 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 localization 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 the range of UWB localization can be up to 2km than  $\sigma < 0.005R$ . Indoor, if ultrasound is used for localization 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 17 and 18, the probability of attacker’s success in these scenarios will then be as low as  $10^{-35}$ .

## VIII. RELATED WORK

In the last decade, a number of indoor localization systems were proposed, based notably on infrared [50], ultrasound [51], [35], received radio signal strength [4], [20], [10] and time-of-flight radio signal propagation techniques [27], [15]. These localization techniques were then extended and used for localization in sensor and ad hoc networks [13], [7], [47], [33], [32], [44], [30], [14].

Recently, a number of secure distance and location verification have been proposed. Brands and Chaum [6] 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 [43] 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 the proposal is based on ultrasound distance bounding, it can be used only for the verification of nodes’ locations, 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 [48] propose a technique called verifiable multilateration, based on distance-bounding, which enables a local infrastructure to verify locations of the nodes. They further show how that technique can be extended for secure localization of a network of sensors. Lazos et al. [26] proposed a set of techniques for secure localization 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. Rasmussen, Capkun and Cagalj propose SecNav [37] that relies on signal broadcasts using I-codes [9] to achieve secure localization and time synchronization. Recently, a number of proposals have been made to protect the anonymity and location privacy of wireless devices [38], [19], [39], [42], [23], [24].

## IX. CONCLUSION

In this work, we proposed a novel approach to secure localization based on covert (hidden and mobile) base stations. This approach enables secure localization with a broad spectrum of localization 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 localization schemes. We have shown how security of this approach depends on the precision of the localization 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 also intend to investigate in more detail the privacy implications of our approach.

## REFERENCES

- [1] Amigobot. <http://www.amigobot.com/>.
- [2] Uwb technology for positioning. [www.thalesresearch.com](http://www.thalesresearch.com).
- [3] 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.
- [4] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, volume 2, pages 775–784, 2000.
- [5] S. Bergbreiter and K. S. J. Pister. CotsBots: An Off-the-Shelf Platform for Distributed Robotics. In *Proceedings of IROS*, 2003.
- [6] 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.
- [7] 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.
- [8] W. F. Butler. Antenna backscatter with applications to surgical countermeasures. Technical Report ADE001679, Defence Technical Information Service, 1981.
- [9] Mario Cagalj, Srdjan Capkun, RamKumar Rengaswamy, Ilias Tsigkogiannis, Mani Srivastava, and Jean-Pierre Hubaux. Integrity (I) codes: Message integrity protection and authentication over insecure channels. In *IEEE Symposium on Security and Privacy (S&P)*, 2006.
- [10] 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.
- [11] 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.
- [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 the IEEE Conference on Computer Communications (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 the IEEE Conference on Computer Communications (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 the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*. ACM Press, 2004.
- [22] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, San Francisco, USA, April 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. Capkun, 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 the IEEE Conference on Computer Communications (InfoCom)*, San Francisco, USA, April 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 the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pages 32–43. ACM Press, 2000.
- [36] Kasper Bonne Rasmussen and Srdjan Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Proceedings of IEEE SecureComm*, 2007.
- [37] Kasper Bonne Rasmussen, Srdjan Capkun, and Mario Galaj. SecNav: Secure broadcast localization and time synchronization in wireless networks. In *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 310–313, New York, NY, USA, 2007. ACM Press.
- [38] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *Pervasive Computing*, January-March 2003.
- [39] I. W. Jackson. Anonymous Addresses and Confidentiality of Location. In *Proceedings of International Workshop on Information Hiding*, 1996.
- [40] M. G. Kendall and P.A.P. Moran. *Geometrical Probability*. Hafner, New York, 1963.
- [41] 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.
- [42] Y.-C. Hu and H. J. Wang. Location Privacy in Wireless Networks. In *Proceedings of the ACM SIGCOMM Asia Workshop*, 2005.
- [43] 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.
- [44] A. Savvides, C.-C. Han, and M. B. Strivastava. Dynamic fine-grained localization in Ad-Hoc networks of sensors. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pages 166–179. ACM Press, 2001.
- [45] S. Sedihpour, S. Capkun, S. Ganeriwal, and M. Srivastava. Implementation of attacks on ultrasonic ranging systems, demo. *SENSYS*, 2005.
- [46] S. Capkun, L. Buttyán, and J.-P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, Washington, USA, October 2003.
- [47] S. Capkun, M. Hamdi, and J.-P. Hubaux. GPS-free Positioning in Mobile Ad-Hoc Networks. *Cluster Computing*, 5(2), April 2002.
- [48] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, 2005.
- [49] S. Capkun, J.-P. Hubaux, and L. Buttyán. Mobility Helps Peer-to-Peer Security. *IEEE Transactions on Mobile Computing*, January 2005.
- [50] R. Want, A. Hopper, V. Falcao, and J. Gibbons. The Active Badge Location system. *ACM Transactions on Information Systems*, 10(1):91–102, 1992.
- [51] A. Ward, A. Jones, and A. Hopper. A New Location Technique for the Active Office. *IEEE Personal Communications*, 4(5), October 1997.