Secure Location Verification with Hidden and Mobile Base Stations

Srdjan Čapkun, *Member, IEEE, IEEE Computer Society*, Kasper Bonne Rasmussen, *Member, IEEE*,
Mario Čagalj, *Member, IEEE*, and Mani Srivastava, *Member, IEEE*

Abstract—In this work, we propose and analyze 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 the 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.

Index Terms—Mobility, location verification, security, wireless networks.

◆

1 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 (that is, position-based routing) to enabling location-related applications (for example, access control and data harvesting).

The proposed techniques were mainly studied in nonadversarial 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, whereas external attackers can spoof measured locations of honest nodes. Localization and ranging techniques in wireless networks mainly rely on measurements of the time of flight of radio (RF ToF) or time of flight of 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 US ToF and those based on the measurements of RF RSS are particularly vulnerable to position spoofing attacks. Systems based on RF ToF measurements are less vulnerable to attacks because of the high speed of signal propagation.

Recently, a number of secure localization techniques have been 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 with ns precision 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 by using any kind of ranging, even low-cost RSSI-based methods (for example, [4], [20], and [10]).

Our approach to secure localization relies on a set of covert base stations (CBSs). By 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, the locations of CBSs represent a secret input (*a key*) to the system. CBSs can be realized by hiding or disguising a static base station or by the random motion of mobile base stations (MBSs). Typically, CBSs are passive.

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

We show through three example protocols how CBSs 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 the security of the proposed protocols depends on the precision of the localization and ranging techniques and on the number of CBSs. We capture this analytically.

The organization of the rest of this paper is given as follows: In Section 2, we present our system model. In Sections 3 and 4, we present protocols for secure localization in infrastructure-centric and node-centric systems, respectively. In Sections 5 and 6, we show how MBSs can be applied to secure localization in sensor and mobile ad hoc networks.

- S. Čapkun and K.B. Rasmussen are with the Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland. E-mail: {capkuns, kasperr}@inf.ethz.ch.
- M. Čagalj is with the Department of Electronics, Faculty of Electrical Engineering, Mechanical Engineering, and Naval Architecture (FESB), University of Split, 21000 Split, Croatia. E-mail: mario.cagalj@fesb.hr.
- M. Srivastava is with the Electrical Engineering Department, University of California, Los Angeles, CA 90095. E-mail: mbs@ucla.edu.

Manuscript received 23 Jan. 2007; revised 23 July 2007; accepted 16 Oct. 2007; published online 6 Nov. 2007.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-0029-0107.
Digital Object Identifier no. 10.1109/TMC.2007.70782.

1536-1233/08/$25.00 © 2008 IEEE Published by the IEEE CS, CASS, ComSoc, IES, & SPS

In Section 7, we analyze our schemes. In Section 8, we review the related work. We conclude this paper in Section 9.

2 MODEL

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

2.1 System Model

Our system consists of a set of CBSs and a set of public base stations (PBS) forming a localization infrastructure. Here, by CBSs, 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, CBSs are silent on the wireless channel: they only listen to the ongoing communication.

In our system, CBSs and PBSs know their locations or can obtain their locations securely and passively (for example, through a secure GPS [25]). Here, we assume that the attackers cannot tamper with these locations or 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 PBS, whereas the hidden stations remain passive.

We further assume that CBSs can measure the received signal strength or have an ultrasonic interface, through which they perform ranging.

In most of this work, we assume that CBSs 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 5, we modify our assumptions. We replace the PBSs and CBSs with MBSs, 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 the nodes from simply trying different distances until they get it right.

2.2 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 (that is, 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 the signals received from PBSs with known locations. If the localization system is *node centric*, internal attacks are generally straightforward: an attacker simply lies about the position that it computed. *Infrastructure-centric* localization systems are those in which the infrastructure computes the 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 (that is, 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 (for example, by using directional antennas).

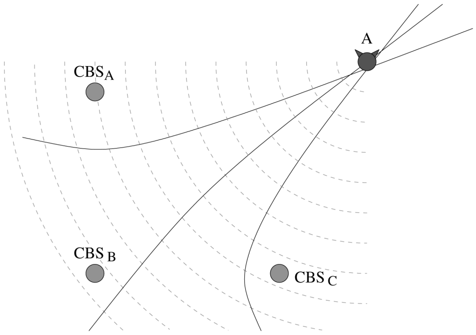


Fig. 1. An example of localization with TDOA. The base stations CBS_A, CBS_B, and CBS_C measure the differences of signal arrival times and computes the position of the attacker. The full lines are the hyperboles found by each pair of base stations.

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.

3 INFRASTRUCTURE-CENTRIC LOCALIZATION WITH HIDDEN BASE STATIONS

In this section, we describe a simple solution for securing infrastructure-centric localization systems based on TDOA and CBSs.

TDOA is the process of localizing the source of a signal in two (respectively, three) dimensions by finding the intersection of multiple hyperbola based on the TDOA between the signal reception at multiple base stations. Using two hyperboles (three base stations), we can obtain 2D device locations, and using three hyperboloids (four base stations), we can determine 3D locations. The operation of the TDOA technique is shown in Fig. 1. Node A sends a radio signal, and the verifiers CBS_A, CBS_B, and CBS_C measure the difference between the signal arrival time 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 by measuring the 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 intersection point of the

PBS $\qquad\qquad\qquad$ A
The nonce N is sent at t_s
$\xrightarrow{N}$
$m = \{A, N, \mathrm{sign}_{K_A}(A, N)\}$
CBS $\qquad\qquad\qquad$ A
$\xleftarrow{m}$
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

Fig. 2. TDOA with hidden base stations.

hyperboles constructed with measured time differences (see Fig. 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 in Fig. 2.

3.1 Security Analysis

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 $h(p^*, i, j)$ 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. 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 pairwise clock drifts of the base stations. T is the time within which a node needs to reply to a challenge issued by a PBS: 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 CBSs 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, whereas an external attacker can jam and delay a node's original messages and thus spoof its location.

With CBSs, 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 the attacker's guessing space. To put it simply, if Δ is large, a false position will be more likely accepted, as the tolerance to inconsistencies will be higher. In Section 7, we investigate in more detail the relationship between Δ and the attacker's success.

In addition, we need to consider one more external attack on TDOA, that is, an external wormhole. This attack is performed as follows: 1) an attacker jams the original localization message m sent by node A and 2) the attacker replays m from a location p'_A. As a result, the base stations will be convinced that node A is located at p'_A, whereas its true position is p_A. In order to mount this attack, the attacker needs to jam all hidden base stations and have faster processing than regular mobile nodes. Finally, in order to show that 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 CBSs, 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 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 those scenarios in which the attacker does not have the ability to perform the described wormhole attack (that is, either it cannot jam the communication between the node and the base station or it does not have fast-processing hardware).

In our protocol, node location privacy is not preserved. However, this protocol can be enhanced to include PBS authentication, which prevents an attacker from challenging the node and from prompting it to send localization signals, disclosing its location. Other attacks are possible on a node's location privacy [38], [19], [39], [42], [23], [24], but coping with these attacks is out of the scope of this paper.

4 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 nonsecure localization system. This position is then reported to the infrastructure comprised of CBSs, 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 the 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 CBS. 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 shown in Fig. 3. Here, N is a nonce generated by the PBS, Δ is a combined localization and

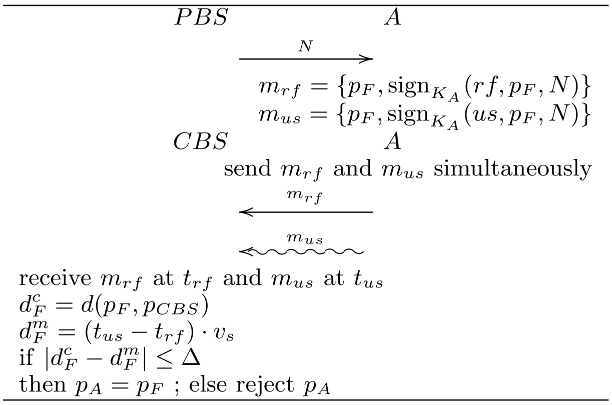


Fig. 3. Position verification with hidden base stations.

ranging error, and T is the time within which a node needs to reply to a challenge issued by a PBS.

In this protocol, the infrastructure uses a PBS to communicate with the node and a single CBS to verify the reported position. The PBS sends a challenge to the node A, which then replies by sending radio and ultrasonic messages containing the alleged node position p_F. The 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, the CBS concludes that p_F is the position of A. An illustration of a fake position report is shown in Fig. 4. To do this, the 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 the two distances differ by more than the expected combined localization and ranging error Δ, then the position is rejected; else, the position is accepted as the 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.

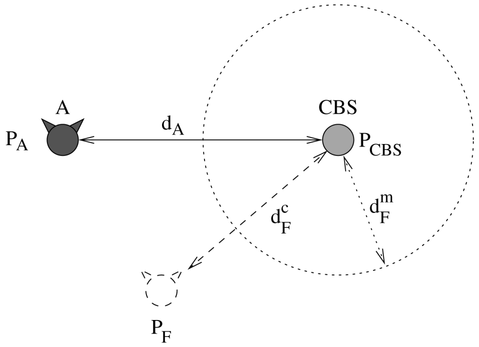


Fig. 4. False position report by node A to the CBS. p_A is the true node position, p_F is the fake node position (reported by A to the CBS), and p_{CBS} is the position of the CBS. $d_F^c = d(p_F, p_{CBS})$ is the (false) distance between the CBS and A computed by the CBS, and d_F^m is the (false) distance between A and the CBS measured passively by the CBS. If $|d_F^c - d_F^m| \leq \Delta$, then $p_A = p_F$.

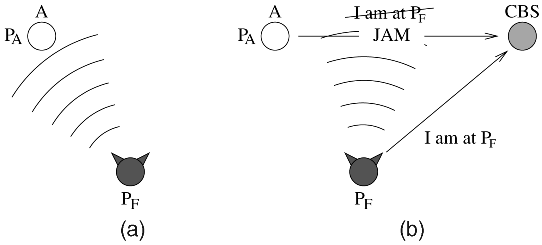


Fig. 5. Position spoofing attack. (a) The attacker spoofs node A into believing that it is at the attackers location P_F (for example, by using a fake GPS station). (b) Then, the attacker jams the localization message and replays it from its own position there by fooling the CBS into accepting the position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

4.1 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 7.

External attacks against position verification are more complex and include position spoofing, jamming, and message replays. Fig. 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 CBS 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.

Similar 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 of 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 PBS 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, for example, 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. Although 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 7).

5 SECURE LOCALIZATION IN SENSOR NETWORKS WITH MOBILE BASE STATIONS

The use of MBSs 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 MBSs for secure localization in sensor networks.

5.1 Scenario

In our scenario, we rely on MBSs. We show how MBSs 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 nonsecure localization algorithms [13], [7], [47], [33], [32], [44], [30], [14], [11].

We further assume that the authority has a number of MBSs (similar to data mules) that know securely their locations (for example, through a secure GPS [25]). These MBSs can be single purpose or multipurpose and therefore can be used not only for position verification but also for data collection and other tasks.

We assume that the MBSs share a secret key with each sensor.

5.2 Position Verification with Mobile Base Stations

The protocol presented in this section is similar to the position verification protocol presented in Section 4. That protocol relied on the assumption that the CBS is hidden, whereas all communication between the node and the localization infrastructure is performed through the PBS.

Here, position verification is performed through MBSs. 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 MBS. In this protocol, the role of a PBS is thus replaced with base station mobility.

MBS $\qquad\qquad$ A

$$\xrightarrow{MBS,N,T_R}$$

$$m_{rf} = \{p, \mathrm{MAC}_K(rf, p, MBS, A, N)\}$$
$$m_{us} = \{p, \mathrm{MAC}_K(us, p, MBS, A, N)\}$$

move to a new location

send m_{rf} and m_{us} simultaneously for the next T_R seconds

$$\xleftarrow{m_{rf}}$$

$$\xleftarrow{m_{us}}$$

receive m_{rf} at t_{rf} and m_{us} at t_{us}

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

$d_A^m = (t_{us} - t_{rf}) \cdot v_s$

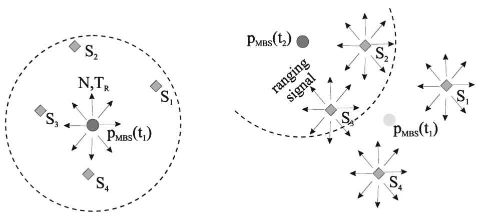
if $|d_A^c - d_A^m| \leq \Delta$ then $p_A = p$; else reject p

Fig. 6. Position verification with MBSs.

Our protocol is shown in Fig. 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 sec. 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. Furthermore, 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 in Fig. 7. At time t_1, an 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, the 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 $p_{MBS}(t_2)$, the MBS receives a reply from the sensors that are still in its power range. Based on the received replies, the 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 4).



(a) (b)

Fig. 7. Position verification in sensor networks. An MBS verifies the locations of nodes. (a) At time t_1, the MBS challenges sensor nodes. (b) At time $t_2 > t_1$, the sensors reply to the challenge, and their locations are verified by MBS.

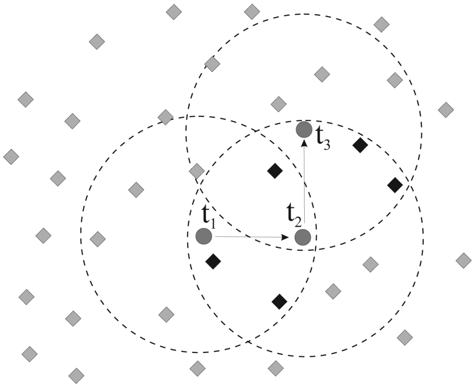


Fig. 8. Progress of position verification in sensor networks with MBSs. An MBS moves from position $p_{MBS}(t_1)$ to $p_{MBS}(t_2)$ and $p_{MBS}(t_3)$.

5.3 Mobile Base Station Coverage and Simulation

Typically, the MBS can perform simultaneous verification of locations of multiple sensors. If at each motion step t_i, the MBS moves within the circle defined by its power range, it will hear at least 39 percent of the sensors that were in its power range at time t_{i-1}, provided that the sensors are uniformly distributed over the MBSs power range.[1] This is because the intersection of the MBSs power ranges at t_1 and at t_2 will be at least 39 percent of the circle surface, given that the MBS moved within its previous power range. At time t_1, the MBS broadcast 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, and then, the MBS moves again and waits for their replies. Hence, as the MBS moves through the network, it will only verify locations of the sensors that were in the intersections of two subsequent power ranges of the MBS. This is illustrated in Fig. 8. The trajectory of the MBS needs to be unpredictable for the sensor nodes, even if the sensors collude. One way of ensuring 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] and [3], the authors provide a set of analytical and simulation results for the 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). Fig. 9 is a plot of the coverage as a function of the movement range. A single MBS moves according to a random walk for 60 seconds in a 500 m × 500 m area with 300 nodes. The four different curves are four different transmission ranges. It is clear in 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 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.

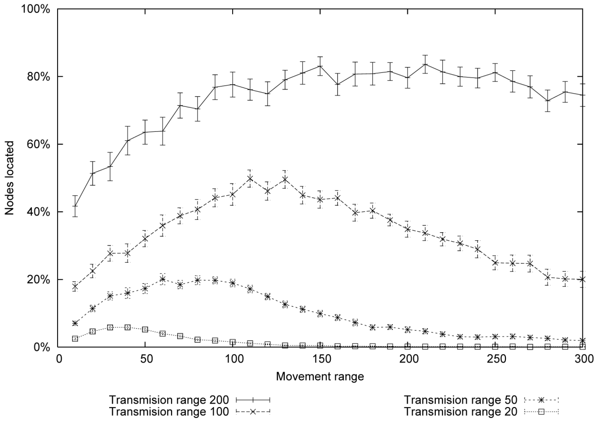


Fig. 9. MBS coverage for different values of transmission and movement range (step size). Every point on the graph is the average result of 50 simulations, whereas the vertical bars indicate the 95 percent confidence interval.

Fig. 10 shows the coverage time of 300 sensors placed randomly throughout an area of 500 m × 500 m. One node is chosen to be an MBS and moves through the network by 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 disk described by its transmission range, and moves there. The speed at which the MBS moves is set to 50 m/s, which is about the speed of a small drone over a battlefield, and the node time-out 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 of the form

$$C = at + b\ln(t) + c \tag{1}$$

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. Using (1), it is possible to estimate the required equipment specifications

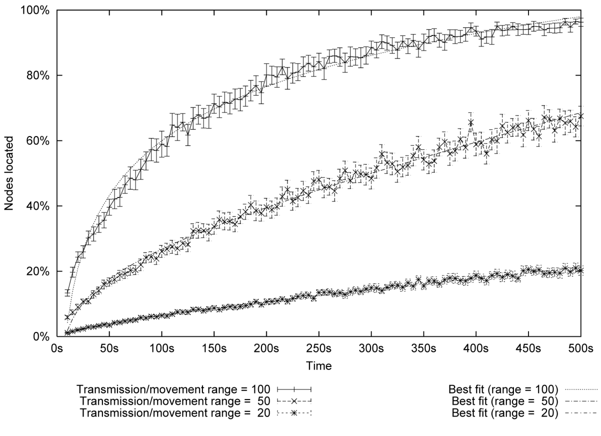


Fig. 10. MBS coverage as a function of time. Every point on the graph is the average result of 50 simulations, whereas the vertical bars indicate the 95 percent confidence interval.

---

[1] This also assumes that either the MBS and the nodes have the same transmission radius or the MBS has a high-gain antenna that will enable it to receive the reply from within its own transmission radius.

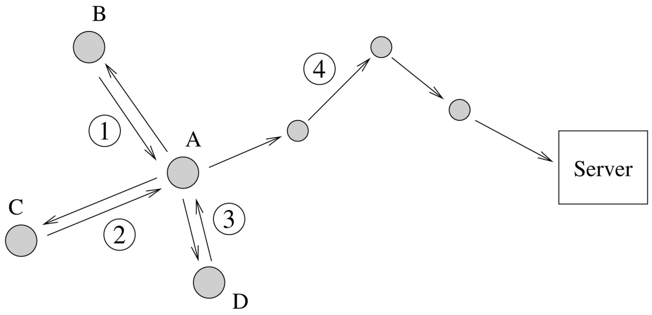


Fig. 11. Node A gathers signed witness statements about its location in order to update a central location database (residing on the server S). Each using the protocol in Fig. 12, nodes B, C, and D first verify the location of A (steps 1, 2, and 3) and then send (to A) signed statements about their locations.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

$$
\begin{array}{rcl}
 & A: & \text{pick } N \leftarrow \{0,1\}^k \\
A \substack{\longrightarrow \\ \leadsto} & *: & A, P_A, T_A, N, \text{sign}_{K_A}\{A, P_A, T_A, N\} \\
 & & \\
 & B: & d_A^c \leftarrow \text{dist}(P_A, P_B) \\
 & & d_A^m \leftarrow (t_{us} - t_{rf}) \cdot v_s \\
 & & \textbf{if } |d_A^c - d_A^m| \leq \Delta \\
 & & \textbf{then } m \leftarrow \text{enc}_{K_{BS}}(B, A, T_B, P_A, ok) \\
 & & \textbf{else } m \leftarrow \text{enc}_{K_{BS}}(B, A, T_B, P_A, nok) \\
 & & stat_B \leftarrow m, \text{sign}_{K_B}\{m, N\} \\
 & & \\
B \longrightarrow & A: & stat_B \\
A \longrightarrow & S: & m
\end{array}
$$

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 and 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.

(that is, the 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 4, and thus, we do not repeat it here.

6 LOCATION VERIFICATION IN MOBILE AD HOC NETWORKS

In this section, we show how our node-centric position verification protocols (Section 4) 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 5 in that there are no dedicated MBSs that move around and localize nodes. Instead, in this scenario, nodes obtain their positions by using a global positioning system (for example, the 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 by assuming that the nodes implement US-based passive ranging, although other passive ranging scheme can be used (for example, RSSI-based ranging).

6.1 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 (for example, 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 Fig. 11.

In order to update its location at the server, node A executes the protocol shown in Fig. 12. A starts the protocol by announcing its location on both the RF and US channels with a signed broadcast message containing its location P_A and the time stamp T_A. A's neighbors (for example, B) verify A's location claim and then issue a time-stamped and signed statement $stat_B$ regarding A's claim. These statements can be either 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 in 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 checks if the nodes' claimed locations and the location statements of their neighbors match. The information collected at the server can then be used by the network nodes, for example, for secure location-based routing, and by the server, for example, 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. Thus, B can do locally by monitoring how much it moved since its last transmission.

6.2 Security Analysis

An attacker that wants to falsify its location must make the distance calculated at the receiver match the position that the attacker reports. We analyze this in detail in Section 7. 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 have discussed above, the proposed protocol preserves a node's privacy from all nodes, except from their neighbors (that need to know the node's location in order to verify it).

7 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 CBSs. 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 4. 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 CBS 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 attacker success is therefore

$$P(|d_F^c - d_F^m| \leq \Delta \mid p_F \neq p_A). \tag{2}$$

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 circles, as they best reflect the power ranges of the devices.

7.1 Attacker's Average Success Probability

To compute the average probability of an 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]

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

for a disk and by

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

for a ball, where R is the radius of the disk/ball. P_D and P_B are shown in Fig. 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

$$P_{D,uni} = \int_{0.84R-\Delta}^{0.84R+\Delta} P_D \,\mathrm{d}d \approx 0.809 \cdot 2\frac{\Delta}{R}, \tag{5}$$

$$P_{B,uni} = \int_{1.05R-\Delta}^{1.05R+\Delta} P_B \,\mathrm{d}d \approx 0.942 \cdot 2\frac{\Delta}{R}. \tag{6}$$

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

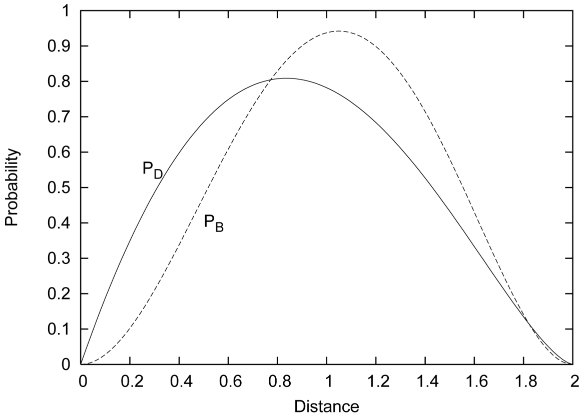


Fig. 13. The pdf of the distance $d_F^c = d(p_F, p_{CBS})$ on a disk P_D and in a ball P_B, when p_{CBS} and p_F are chosen uniformly over the disk and ball, respectively.

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

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

$$P^n_{B,uni} \approx \left(0.942 \cdot 2\frac{\Delta}{R}\right)^n. \tag{8}$$

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

7.2 Attacker's Maximum Success Probability

So far, we have assumed that the attacker's position p_A is chosen uniformly, meaning 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 $Pmax$ if he chooses his position p_A at the center of the disk/ball and if he chooses $d_F^m = R - \Delta$ as his fake measured distance to CBS. This probability is given as follows (for a disk):

$$\begin{aligned} P_D(d_A \leq d) &= \frac{\pi d^2}{\pi R^2}, \\ P_D(d_A = d \pm \Delta) &= \frac{\pi(d+\Delta)^2 - \pi(d-\Delta)^2}{\pi R^2} \\ &= \frac{4d\Delta}{R^2}, \\ Pmax_D &= P_D(d_A = (R-\Delta) \pm \Delta) \\ &= \frac{4\Delta(R-\Delta)}{R^2}. \end{aligned} \tag{9}$$

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 CBSs, is

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

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

This analysis shows that in the worst case scenario, the maximum probability of the attacker's success is approximately 2.5 times (disk, 2D) and 3 times (ball, 3D) the average probability of the 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 disk/ball is the set of points on a circle (sphere) of radius R when p is at the center of a disk/ball.

7.3 Extending the Analysis to Time Difference of Arrival

In the case of position verification using TDOA as described in Section 3, there is one additional element that the attacker must consider. If the attacker will 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 the case when the attacker positions himself at the center of the verification circle.

If the CBSs are randomly distributed across the verification space, the probability of the attacker hitting the correct CBS depends on the angle of his transmission cone. If the angle θ is 0 degree, the probability of hitting the correct base station is also 0. If the angle is θ_{max} (that is, 360 degrees in a full circle), then the probability of hitting the correct CBS is 1. We can write the following relation between the probability and angle:

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

where θ is the absolute angle, and θ_{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 CBSs. 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 (that is, a minimum of 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, that is, the maximum of $P_{hit} \cdot P_{mtr}$. It is straightforward to show that the maximum of $P_{hit} \cdot P_{mtr}$ is $\frac{1}{n}$.

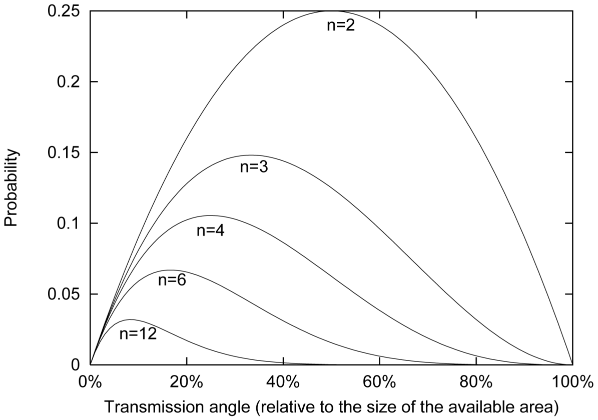


Fig. 14. The probability of successfully guessing the direction of one of the CBSs while at the same time not hitting any of the other base stations $P_{hit} \cdot P_{mtr}$. Note that the angle is relative to the size of the guessing space.

In Fig. 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 in Fig. 14 that the attacker would pick a transmission cone width of 1/4 of the guessing space or $\theta = 90$ degrees, giving a probability of successfully guessing the direction of one of the CBS while at the same time not hitting anyone else by 10.5 percent. However, 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 degrees to $360 \text{ degrees} - 90 \text{ degrees} = 270 \text{ degrees}$, and the number of base stations is reduced from 4 to 3. Because there are now only three base stations, the attacker will chose an angle of 1/3 of the remaining guessing space or 90 degrees. This gives a probability of successfully guessing the direction of another CBS while at the same time not hitting any of the other stations by 14.8 percent. Now, the guessing space is further reduced to $270 \text{ degrees} - 90 \text{ degrees} = 180 \text{ degrees}$, and the number of base stations is 2. Choosing $\theta = 90 \text{ degrees}$ (half the guessing space), the probability is 25 percent. After this, there is only one CBS left, and 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 CBSs without accidentally hitting any wrong CBS is therefore

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

This example is illustrated in Fig. 15.

Following the above procedure, it is easy to see that the combined probability of correctly aiming N directional antennas at N CBSs 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 CBSs in the verification space.

It should be clarified that this probability only covers the aiming of the antennas. If an attacker actually wants to

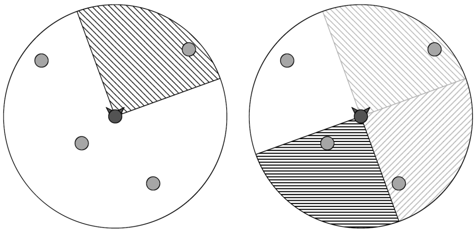


Fig. 15. An example of an attacker guessing the directions to four CBSs in such a way that a transmission to any of the CBSs would not be received by any other CBS.

cheat on a location in a TDOA environment, he must also fake the distance to each of the CBSs. 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

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

7.4 Further Reducing the Probability of Attacker's Success

The attacker's success can be further reduced by increasing the space in which the CBSs 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 CBSs are positioned. However, the CBSs can also be placed outside the localization region (around the localization region). The maximal distance from the CBSs 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 in Fig. 16. In this case, the maximum probability of the 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 the 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 obtaining information about the location of a mobile or CBS by using a radar-based system capable of detecting antenna backscatter (that is, the energy that is reradiated by a receiving antenna). However, this energy is very weak compared to the original signal, and the radar signature that it generates is not 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 (for example, urban) environments.

7.5 Sensitivity

In this section, we analyze the frequency of false positives and false negatives as a function of the expected localization 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 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 Δ 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 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 localization and ranging errors.

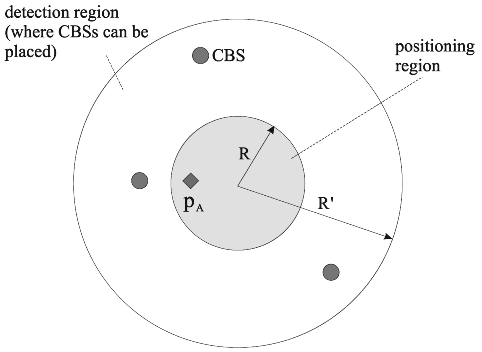


Fig. 16. Localization and detection region. If the base stations can be positioned outside the localization zone, the probability of the attacker's success can be further decreased.

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 $error_R \sim N(0, \sigma_R^2)$, then 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 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:

$$\Delta = k\sigma, \tag{15}$$

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 the $error$ is Gaussian, the probability that $d_F^c - d_F^m$ falls within the interval $[-k\sigma, k\sigma]$ is given by [34]

$$\begin{aligned} P(-k\sigma < d_F^c - d_F^m < k\sigma) &= \frac{2}{\sqrt{\pi}} \int_0^{\frac{k}{\sqrt{2}}} e^{-u^2} \mathrm{d}u \\ &= \mathrm{erf}\left(\frac{k}{\sqrt{2}}\right). \end{aligned} \tag{16}$$

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

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

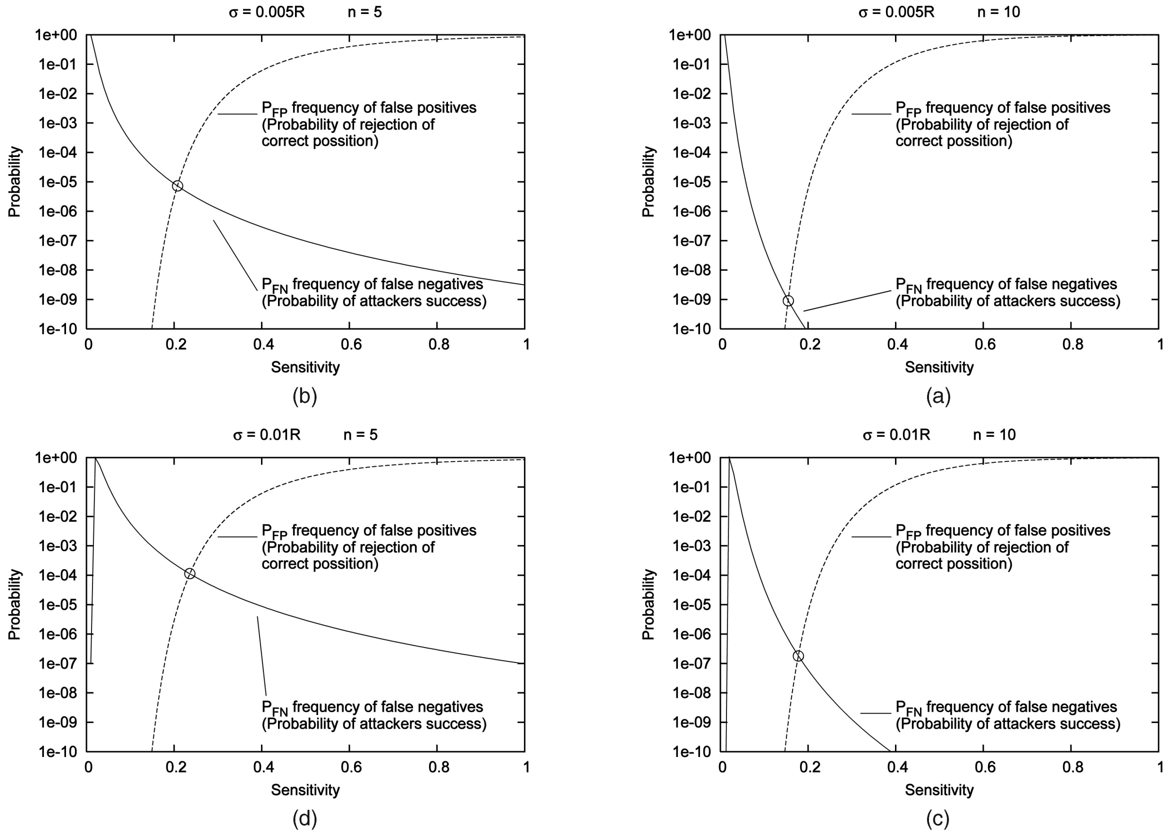


Fig. 17. The frequency of false positives and false negatives, and a crossover error rate for (a) $\sigma = 0.005R$ and $n = 5$, (b) $\sigma = 0.005R$ and $n = 10$, (c) $\sigma = 0.01R$ and $n = 5$, (d) $\sigma = 0.01R$ and $n = 10$. $s = 1/k$ is the sensitivity. $\Delta = k\sigma$ is the tolerated localization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

that is, 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)

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

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

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

Similarly, the frequency of false negatives for n CBSs 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 the attacker's success for n CBSs:

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

Fig. 17 shows 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 the position verification is to errors. If $s = \infty$, the system is very sensitive, and localization and ranging errors will not be tolerated. If $s = 0$, the system tolerates any error. Consequently, the frequencies of false positives and false negatives depend on s.

Fig. 17 shows the frequencies of false positives and false negatives for 5 and 10 CBSs and for $\sigma = 0.005R$ (0.5 percent of R) and $\sigma = 0.01R$ (1 percent 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 is equal to the frequency of false negatives. In these figures, we observe, as expected, that with the increase in the number of CBSs and with the reduction of the standard deviation of the localization and ranging error σ, the crossover error rate can be significantly reduced. If the number of CBSs is $n = 5$ and if $\sigma = 0.01R$, the crossover error rate will be about 1×10^{-4}. This error rate is significantly reduced to approximately 1×10^{-9} if the σ is reduced to $0.005R$ and if the number of CBSs 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 Fig. 18 the probability of false negatives (probability of the attacker's success) as a function of the number of CBSs, given that the frequency of false positives is set to 1 percent. This figure shows that with the frequency of false positives set to 1 percent, the probability of the attacker's success is significantly lower than the crossover error rate. We therefore observe that with five or more CBSs, the probability of the attacker's success is lower than 10^{-5}, with the standard deviation of error smaller than $0.03R$.

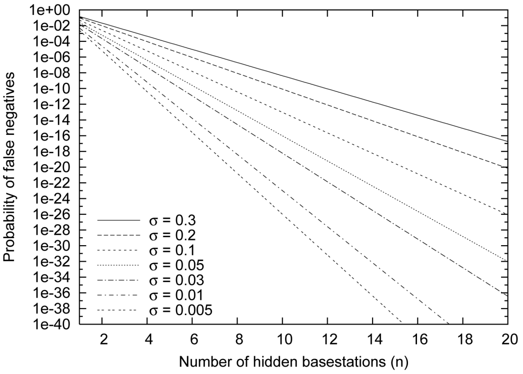


Fig. 18. The frequency of false negatives (the probability of the attacker's success) if the frequency of false positives is set to 1 percent.

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

7.6 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 adopted to work with CBSs. 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 CBSs.

If localization is based on GPS, the accuracy of the localization will be in 95 percent of cases better than 1 m. RF ToF techniques being developed for localization GSM and CDMA position aim at providing accuracy of 50-100 and 10 m in the case of UL-TOA, GSM and AGPS, and CDMA, respectively. Note here that these systems are designed for area and cell sizes that can have radii of 500 m (in highly dense urban areas) to 35 km (in the countryside). Indoors, localization with Wi-Fi based on signal strength measurements with location fingerprinting can achieve localization accuracy of 2-3 m, whereas ultrasound-based ranging and localization systems can be accurate down to a few centimeters. Ultrawideband (UWB) time-of-flight based systems work both indoors and outdoors [2]. Indoors, they can achieve ranging precision better than 1 m for ranges of up to 50 m and localization accuracy of up to 15 cm. The outdoor accuracy of UWB localization and ranging systems can be also very high, approximately 1 m for distances of up to 2 km [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 the 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 m. Given that the range of UWB localization can be up to 2 km than $\sigma < 0.005R$. Indoors, if ultrasound is used for localization and ultrasonic ranging is for verification, we can assume the standard deviation of error to be in the order of 20 centimeters and ranges up to 20 m, meaning that $\sigma = 0.01R$. As we have shown in Figs. 17 and 18, the probability of the attacker's success in these scenarios will then be as low as 10^{-35}.

8 RELATED WORK

In the last decade, a number of indoor localization systems were proposed based notably on infrared [50], US ToF [51], [35], RF RSS [4], [20], [10], and RF ToF 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 schemes 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 et al. [43] proposed a new distance-bounding protocol based on ultrasound and radio wireless communication. In that work, the authors also propose making 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], Hu et al. 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]. Čapkun and Hubaux [48] propose a technique called verifiable multilateration based on distance bounding, which enables a local infrastructure to verify the 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 the consistency of received beacons. Rasmussen et al. 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].

9 CONCLUSION

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

ACKNOWLEDGMENTS

The work presented in this paper was supported (in part) by the Swiss National Science Foundation under Grant 200021-116444/1.

REFERENCES

[1] *Amigobot,* http://www.amigobot.com/, 2007.

[2] *UWB Technology for Positioning,* www.thalesresearch.com, 2007.

[3] C. Avin and C. Brito, "Efficient and Robust Query Processing in Dynamic Environments Using Random Walk Techniques," *Proc. Third Int'l Symp. 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," *Proc. IEEE INFOCOM '00,* vol. 2, pp. 775-784, 2000.

[5] S. Bergbreiter and K.S.J. Pister, "CotsBots: An Off-the-Shelf Platform for Distributed Robotics," *Proc. IEEE/RSJ Int'l Conf. Intelligent Robots and Systems (IROS),* 2003.

[6] S. Brands and D. Chaum, "Distance-Bounding Protocols," *Advances in Cryptology—Proc. Workshop Theory and Application of Cryptographic Techniques (EUROCRYPT '94),* pp. 344-359, 1994.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-Less Low-Cost Outdoor Localization for Very Small Devices," *IEEE Personal Comm. Magazine,* vol. 7, no. 5, pp. 28-34, Oct. 2000.

[8] W.F. Butler, "Antenna Backscatter with Applications to Surgical Countermeasures," Technical Report ADE001679, Defense Technical Information Service, 1981.

[9] M. Cagalj, S. Capkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava, and J.P. Hubaux, "Integrity (I) Codes: Message Integrity Protection and Authentication over Insecure Channels," *Proc. IEEE Symp. 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," *Proc. Third Int'l Conf. Ubiquitous Computing (UbiComp '01),* vol. 2201, Sept. 2001.

[11] H. Chan, M. Luk, and A. Perrig, "Using Clustering Information for Sensor Network Localization," *Proc. First IEEE Conf. Distributed Computing in Sensor Systems (DCOSS '05),* June 2005.

[12] K. Dantu, M.H. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. Sukhatme, "Robomote: Enabling Mobility in Sensor Networks," *Proc. Fourth Int'l Conf. Information Processing in Sensor Networks (IPSN),* 2005.

[13] L. Doherty, K. Pister, and L. El Ghaoui, "Convex Position Estimation in Wireless Sensor Networks," *Proc. IEEE INFOCOM '01,* Apr. 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," *Proc. IEEE 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," *Proc. Second IEEE Conf. Ultra Wideband Systems and Technologies (UWBST '03),* Nov. 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," *Proc. First IEEE Int'l Conf. Distributed Computing in Sensor Systems (DCOSS),* 2005.

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

[19] M. Gruteser and D. Grunwald, "Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: A Quantitative Analysis," *Proc. First ACM Int'l Workshop Wireless Mobile Applications and Services on WLAN Hotspots (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, Univ. of Washington, 2000.

[21] L. Hu and D. Evans, "Localization for Mobile Sensor Networks," *Proc. ACM/IEEE MobiCom,* 2004.

[22] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *Proc. IEEE INFOCOM '03,* Apr. 2003.

[23] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," *Proc. IEEE Wireless Comm. and Networking Conf. (WCNC),* 2005.

[24] J. Kong and X. Hong, "ANODR: ANonymous On-Demand Routing with Untraceable Routes for Mobile Ad Hoc Networks," *Proc. ACM MobiHoc,* 2003.

[25] M.G. Kuhn, "An Asymmetric Security Mechanism for Navigation Signals," *Proc. Sixth Information Hiding Workshop (IH),* 2004.

[26] L. Lazos, S. Čapkun, and R. Poovendran, "ROPE: Robust Position Estimation in Wireless Sensor Networks," *Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN),* 2005.

[27] J.-Y. Lee and R.A. Scholtz, "Ranging in a Dense Multipath Environment Using an UWB Radio Link," *IEEE J. Selected Areas in Comm.,* vol. 20, no. 9, Dec. 2002.

[28] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," *Proc. Fourth Int'l Conf. Information Processing in Sensor Networks (IPSN),* 2005.

[29] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," *Proc. Fourth Int'l Conf. 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," *Proc. Second ACM Conf. Embedded Networked Sensor Systems (SenSys '04),* pp. 50-61, 2004.

[31] L. Navarro-Serment, R. Grabowski, C. Paredis, and P.K. Khosla, "Modularity in Small Distributed Robots," *Proc. SPIE Conf. Sensor Fusion and Decentralized Control in Robotic Systems II,* 1999.

[32] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) Using AOA," *Proc. IEEE INFOCOM '03,* Apr. 2003.

[33] D. Niculescu and B. Nath, "DV-Based Positioning in Ad Hoc Networks," *J. Telecommunication Systems,* vol. 22, no. 4, pp. 267-280, 2003.

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

[35] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," *Proc. ACM/IEEE MobiCom '00,* pp. 32-43, 2000.

[36] K. Rasmussen and S. Capkun, "Implications of Radio Fingerprinting on the Security of Sensor Networks," *Proc. Third IEEE Int'l Conf. Security and Privacy for Comm. Networks (SecureComm),* 2007.

[37] K. Rasmussen, S. Capkun, and M. Cagalj, "SecNav: Secure Broadcast Localization and Time Synchronization in Wireless Networks," *Proc. ACM MobiCom '07,* pp. 310-313, 2007.

[38] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," *Pervasive Computing,* Jan.-Mar. 2003.

[39] I.W. Jackson, "Anonymous Addresses and Confidentiality of Location," *Proc. First Int'l Workshop Information Hiding (IH),* 1996.

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

[41] R.C. Shah, S. Roy, S. Jain, and W. Brunette, "Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks," *Proc. First IEEE Workshop Sensor Network Protocols and Applications (SNPA '03),* May 2003.

[42] Y.-C. Hu and H.J. Wang, "Location Privacy in Wireless Networks," *Proc. ACM SIGCOMM,* 2005.

[43] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," *Proc. ACM Workshop Wireless Security (WiSe '03),* pp. 1-10, Sept. 2003.

[44] A. Savvides, C.-C. Han, and M.B. Strivastava, "Dynamic Fine-Grained Localization in Ad Hoc Networks of Sensors," *Proc. ACM/IEEE MobiCom '01,* pp. 166-179, 2001.

[45] S. Sedihpour, S. Capkun, S. Ganeriwal, and M. Srivastava, "Implementation of Attacks on Ultrasonic Ranging Systems," *Proc. Third ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys),* 2005.

[46] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multihop Wireless Networks," *Proc. First ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '03),* Oct. 2003.

[47] S. Čapkun, M. Hamdi, and J.-P. Hubaux, "GPS-Free Positioning in Mobile Ad Hoc Networks," *Cluster Computing,* vol. 5, no. 2, Apr. 2002.

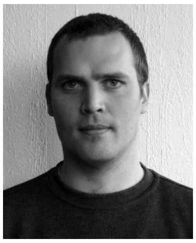
[48] S. Čapkun and J.-P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," *Proc. IEEE INFOCOM,* 2005.

[49] S. Čapkun, J.-P. Hubaux, and L. Buttyán, "Mobility Helps Peer-to-Peer Security," *IEEE Trans. Mobile Computing,* Jan. 2005.

[50] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The Active Badge Location System," *ACM Trans. Information Systems,* vol. 10, no. 1, pp. 91-102, 1992.

[51] A. Ward, A. Jones, and A. Hopper, "A New Location Technique for the Active Office," *IEEE Personal Comm.,* vol. 4, no. 5, Oct. 1997.

Srdjan Čapkun received the DiplIng degree in electrical engineering and computer science from the University of Split, Croatia, in 1998 and the PhD degree in communication systems from the Swiss Federal Institute of Technology of Lausanne (EPFL) in 2004. He is currently an assistant professor in the Department of Computer Science, ETH Zurich. Prior to joining ETH Zurich, he was a postdoctoral researcher in the Networked and Embedded Systems Laboratory (NESL), University of California, Los Angeles, and an assistant professor in the Informatics and Mathematical Modeling Department, Technical University of Denmark (IMM DTU). His research interests include the design and analysis of security protocols for wireless and wireline networks. He is a member of the IEEE and the IEEE Computer Society.



Kasper Bonne Rasmussen received the MSc degree in information technology and mathematics from the Technical University of Denmark in 2005. He is currently working toward the PhD degree with the System Security Group, Department of Computer Science, ETH Zurich. His PhD research focuses on the security of wireless networks, with a special interest in location and time synchronization issues. He is a member of the IEEE.

Mario Čagalj received the DiplIng degree in computer science and electrical engineering from the University of Split, Croatia, in 1998 and the predoctoral and PhD degrees in communication systems from the Ecole Polytechnique Fédérale de Lausanne (EPFL) in 2001 and February 2006, respectively. From 2001 to 2006, he was a research assistant in the Laboratory for Computer Communications and Applications (LCA), EPFL. In January 2006, he joined the Faculty of Electrical Engineering, Mechanical Engineering, and Naval Architecture (FESB), University of Split, where he is currently an assistant professor in the Department of Electronics. His research interests include the design and analysis of security protocols for wireless and wired networks, the application of game theory to communication networks, and the design of energy-efficient communication protocols for wireless networks. He is a member of the IEEE.

Mani Srivastava was born in Lucknow, India. He received the BTech degree in electrical engineering from IIT, Kanpur, India, in 1985 and the MS and PhD degrees from the University of California, Berkeley. His graduate work was focused on CAD tools for embedded DSP VLSI and system designs. His MS project was focused on CMOS bit-slice data path compilation as part of the Lager silicon compiler for DSP VLSI, whereas his PhD dissertation was focused on hardware-software rapid prototyping and codesign at the board level for embedded DSP and control applications. In 1997, he joined the faculty of UCLA, where he is currently a professor and the vice chair of graduate affairs in the Electrical Engineering Department, with a joint appointment as a professor in the Computer Science Department. Before joining UCLA, for about four and a half years, he was with the Networked Computing Research Department, Bell Laboratories, Murray Hill, N.J. (formerly known as AT&T Bell Laboratories and later named Lucent Technologies-Bell Labs Innovations), where his group built one of the first wireless ATM systems. He is currently the editor in chief of the *ACM Mobile Computing and Communications Review* and an associate editor for the *ACM Transactions on Sensor Networks* and the *ACM/IEEE Transactions on Networking.* His research interests include mobile and wireless systems. He is a member of the IEEE.