Guaranteeing the Authenticity of Location Information

A comprehensive definition of location authentication and a review of its threats and possible solutions help provide a better understanding of this young security requirement.

New and enhanced location-determination technologies have allowed ubiquitous computing applications to better exploit location information. In particular, these technologies have improved location-based services, such as emergency and navigation services, tracking and monitoring systems, and location-based billing services. They also apply to more specific contexts—for example, in sensor networks, location information is often crucial for node tracking and packet routing.

This increasing use of location information has driven researchers to analyze its specific security requirements.1 The most important requirements relate to privacy and trust, including authenticity and attestation. Here, we focus on authenticating location information, which is necessary when using such information to grant access to a service or to generate evidence such as a certificate guaranteeing an entity’s location at some point in time. It’s also useful for accountable tracking of nodes and billing of mobile services. More important, for some services—such as emergency related services—failing to guarantee location information can have fatal consequences.

Location authentication is still a relatively young security property. Stefan Brands and David Chaum first addressed location authentication in 1994,2 followed by Dorothy Denning and Peter MacDoran in 1996.3 Researchers have since increased their efforts to understand location authentication, proposing several solutions for different contexts. Despite the recent advances, we still need a clearer picture of this property. Here, we extend a survey we published in 20054 to provide a more comprehensive definition of location authentication and to describe its main threats in different scenarios. We also give an overview of proposed mechanisms for fulfilling this requirement, taking into account not only location verification but also the related problem of secure location determination.

Location determination

We start with a brief overview of location determination because of its obvious importance to location authentication. One main approach to location determination is to use an object’s internal measurements, such as inertial navigation or odometry techniques. However, the more common approach in ubiquitous computing is to use a reference system that exploits triangulation, proximity, or scene-analysis techniques.5

Typically, reference-based location determination considers the exchange of signals between a target node (the one being located) and a set
of reference nodes. Reference nodes are part of a location-determination infrastructure, and they usually either know their location because it’s fixed or can easily determine it.

Reference-based location determination uses either range-dependent or range-independent techniques. Range-dependent techniques measure specific properties of the exchanged signals—properties that depend on the distance between the nodes. Usually, these techniques rely on the signal’s angle of arrival, the received signal strength (RSS), and the propagation time. Range-independent techniques don’t measure signal property; they use other characteristics to determine proximity. For example, they might receive information that the reference nodes (beacons) have broadcast, count the number of hops a message must go through, or identify their location through physical contact with other nodes.

Reference-based location determination also relies on a wireless communication network that’s either infrastructure-based (for example, based on a satellite, cellular, or RFID system) or ad hoc (for example, based on sensor networks). Additionally, it considers the number of reference nodes involved and the kind of signal used (mainly radio and infrared electromagnetic signals or ultrasound signals). Finally, reference-based location determination also considers who estimates the location. In terminal-based schemes, the target node computes its own location, and in infrastructure-based schemes, other nodes, mainly reference nodes, compute the node’s location. Moreover, it could consider who collects the data for computing the location in addition to who performs the computation, but this is less common.

Location authentication
Authentication is widely known in its two major facets. Entity authentication helps corroborate the veracity of a claimed or presumed party’s identity. Data-origin authentication verifies a message’s source. Location authentication assures the truthfulness of the claimed or presumed location information.

The location-authentication schemes we address here use reference-based location determination, so they consider the located node’s information to establish its truthfulness. Reference nodes are also involved in location-authentication schemes, and sometimes a central authority (which might or might not be a reference node) is involved as well.

Because location authentication is a novel security service, the academic community has yet to agree on a common definition. These approaches can use range-dependent or range-independent techniques and are usually infrastructure based. (We distinguish between infrastructure- and terminal-based schemes according to which entity or entities perform the location authentication, not the location estimation.)

Secure location determination
Secure location determination aims to not only determine a target node’s location but also provide some guarantee about the location estimation’s authenticity. Secure location determination thus addresses the authenticity of location information but emphasizes that the location information is known before the execution of the location-determination protocol.

Secure-location-determination protocols can be infrastructure or terminal based, as well as range dependent or range independent. The settings for some infrastructure-based location-determination protocols are similar to those of absolute-location-verification protocols, except that the location information is known or presumed beforehand.

Redefining location authentication
Taking into account location verification and secure location determination, we propose the following

Because location authentication is a novel security service, the academic community has yet to agree on a common definition.

Location verification
 Researchers now commonly refer to Kindberg and Zhang’s definition of location authentication as location verification, emphasizing that the goal is to verify a claimant node’s location. In our setting, the claimant is the target node, and one or more reference nodes or a central authority play the verifier role.

Researchers are addressing different variants of the location-verification problem, using three approaches:

- Distance bounding. This verifies that the claimant’s distance from a certain verifier has an upper bound (that is, the claimant is closer to the verifier than some distance).
<table>
<thead>
<tr>
<th>Location-authentication property</th>
<th>Approach</th>
<th>Proposal</th>
<th>Location-determination technique</th>
<th>No. of reference nodes</th>
<th>Network or system support</th>
<th>Signal used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location verification</td>
<td>Distance bound</td>
<td>Distance-bounding protocols(^2)</td>
<td>ToA(^\star) (round trip)</td>
<td>1</td>
<td>Contactless access-control cards</td>
<td>Signals with light-propagation speed</td>
</tr>
<tr>
<td></td>
<td>Secure and private proofs of location—proximity-proving protocol(^9)</td>
<td>ToA (round trip)</td>
<td>1</td>
<td>Wireless local area network</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distance-bounding proof of knowledge(^10)</td>
<td>ToA (round trip)</td>
<td>1</td>
<td>Contact-based devices</td>
<td>Optical or electrical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RFID distance-bounding protocol(^11)</td>
<td>ToA (round trip)</td>
<td>1</td>
<td>RFID tokens such as contactless smartcards</td>
<td>Radio (ultra-wideband communication)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Symmetric key-based distance-bounding protocol(^12)</td>
<td>ToA (round trip)</td>
<td>1</td>
<td>RFID tokens such as contactless smartcards</td>
<td>Heat and electromagnetic emanations (side-channel leakage)</td>
<td></td>
</tr>
<tr>
<td>In region</td>
<td>Secure verification of location claims(^13)</td>
<td>ToA (round trip)</td>
<td>Multiple (acceptors)—only one executes the protocol</td>
<td>Sensor and wireless networks</td>
<td>Radio and ultrasound</td>
<td></td>
</tr>
<tr>
<td>Absolute location</td>
<td>Location-based authentication system(^3)</td>
<td>Location signatures (specific differential GPS)</td>
<td>Multiple (all in view)</td>
<td>Satellite network (GPS)</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure and private proofs of location—absolute-position verification(^8)</td>
<td>ToA (round trip)</td>
<td>Multiple</td>
<td>Wireless local area networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Verifiable multilateration(^14)</td>
<td>ToA (round trip)</td>
<td>Multiple</td>
<td>Wireless networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td>Location determination</td>
<td>Infrastructure based</td>
<td>Trusted GNSS(^7) receivers(^15)</td>
<td>ToA (one way)</td>
<td>Satellite network (GNSS)</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asymmetric security mechanism for navigation signals(^16)</td>
<td>ToA (one way)</td>
<td>Multiple</td>
<td>Satellite network (GNSS)</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure positioning with direct sensor positioning(^14)</td>
<td>ToA (round trip)</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td>Terminal based</td>
<td>Attack resistant minimum-mean-square location estimation(^17)</td>
<td>Compatible techniques (such as RSSI(^F))</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Voting-based location estimation(^17)</td>
<td>Compatible techniques (such as RSSI)</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Robust statistical method for triangulation(^18)</td>
<td>Any range-dependent technique</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure positioning in sensor networks(^14)</td>
<td>ToA (round trip)</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
</tbody>
</table>

* Time of arrival, † Global Navigation Satellite System, ‡ Received signal strength indication
### Location-authentication property

<table>
<thead>
<tr>
<th>Location-authentication property</th>
<th>Approach</th>
<th>Proposal</th>
<th>Location-determination technique</th>
<th>No. of reference nodes</th>
<th>Network or system support</th>
<th>Signal used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location verification (infrastructure based)</td>
<td>Distance bound</td>
<td>Location-authentication protocols</td>
<td>Proximity (in range)</td>
<td>1</td>
<td>Wireless networks</td>
<td>Radio (short-range communication technology)</td>
</tr>
<tr>
<td>In region</td>
<td>Secure location verification using radio broadcast</td>
<td>Proximity (in range)</td>
<td>Multiple (acceptors and rejectors)</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td>Location determination (infrastructure based)</td>
<td>Secure localization using transmission-rate variation</td>
<td>Proximity (in range)</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td>Terminal based</td>
<td>Secure range-independent localization</td>
<td>Proximity (in range)</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
</tr>
<tr>
<td>Secure localization with attack tolerance</td>
<td>Proximity (in range)</td>
<td>Multiple</td>
<td>Sensor networks</td>
<td>Radio</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Underlying location-determination techniques

Most range-dependent location-authentication techniques are built on time-based location determination techniques; the rest use RSS techniques. Time-based techniques estimate the distance between two nodes using a signal with a relatively constant propagation speed to transmit messages. Then, the time a message sent by one node takes to reach the other node (one-way time) is measured, or the time for the first node to receive a response to its message from the other node (round-trip time) is measured. The total latency usually includes the nodes’ processing time, though it’s considered negligible in most cases. Satellite-based systems also use differential techniques (differential GPS) to enhance location-estimation precision by mitigating undesirable deviations in the satellite signals (these deviations are estimated by nodes that know their own location).

RSS-based techniques use a signal that’s altered depending on its travelled distance. Some location-authentication techniques use RSS indication, which estimates distance directly from the attenuation.

Most range-independent location-authentication schemes use proximity-based techniques, which assume that if a node broadcasts a message, only other nodes close to the transmitting node (within its range) will receive the message.

In all these techniques, when three or more reference nodes are involved, triangulation can be applied to estimate an absolute position. Figure 1 shows an overview of the location-authentication settings we’ve identified according to their underlying location-estimation technique.

### Location-authentication threat models

Only a few location-authentication schemes have been industrially deployed, so the threat models researchers have addressed are somewhat theoretical. After analyzing most location-authentication schemes, we’ve identified two different threat models. The first applies to infrastructure-based location-authentication schemes; the second one to terminal-based schemes.

Both models usually consider the attacker to be an active adversary. The attacker can capture, record, intercept, replay, or insert any message in the communication medium using any kind of signal. We call the...
The model for infrastructure-based schemes

In infrastructure-based schemes, the adversary’s goal is to make reference nodes incorrectly verify or determine the target node’s location at some point in time. This goal includes several threats that result if one or more of the elements in the tuple \((id, l, t)\) is incorrectly verified or computed—where \(id\) stands for node identification, \(l\) for location, and \(t\) for time.

For example, the adversary might try to make a verifier believe that a node identified as \(id\) is at a different location \(l\) than it really is by using a node \(id\) placed at \(l\). Then the verifiers might think that a different node \(id\) is at \(l\). Infrastructure-based schemes assume that the reference nodes can be trusted and that they usually can communicate securely with a central authority.

The model for terminal-based schemes

In terminal-based schemes, the adversary’s goal is for the target node to incorrectly compute its own location at some moment. In this case, we assume that the reference nodes are either malicious or compromised.

Attacks and solutions

Researchers are addressing a set of known attacks for various location-authentication settings. Most attacks target the location information, although others target the time of the location authentication or the located node’s identity. Here, we briefly describe the attacks (see Table 3) and analyze...
how existing location-authentication schemes address them.

**Impersonation**
An external node E or a malicious node T* might try to impersonate an honest node T to make the reference nodes R or the central node C believe that T is at target location l when actually E or T* is located there.

To prevent this attack, the scheme must authenticate the target node during the protocol execution.

**Distance fraud**
An attacker controlling a malicious target node T* might try to manipulate the device or make it so that it no longer follows the protocol’s rules and thus makes the verifiers believe that T* is closer to them than it really is. In schemes based on round-trip time of arrival (ToA), the adversary might undertake this attack by sending the response in advance or manipulating the device’s clock speed. In other cases, the adversary might try to manipulate the node to generate fake reports about its location or manipulate the captured signals.

**Absolute-location fraud**
An attacker controlling a malicious node T* might try to make the verification or determination of its absolute location by manipulating the device or make it so that it no longer follows the protocol’s rules. Then, reference nodes or the central node might believe that T* is in a different location than it is. In schemes based on multi-lateration, the adversary might undertake this attack by making some of the reference nodes (falsely) believe that the adversary is farther away than it really is. Distance-bounding protocols don’t aim to prevent this action. In other cases, the adversary might try to manipulate the node to generate fake reports about its location or manipulate the captured signals.

This attack is prevented in round-trip-TOA-based techniques if the target node is within the polygon or polyhedron formed by the involved reference nodes. In proximity-based schemes, tokens should be unrelated to the distance they address. This hinders malicious nodes from selecting a coherent set of tokens that result in a false location estimation. Other schemes require tamper-resistant devices to prevent target nodes from manipulating signals received from reference nodes or creating fake reports.

**Table 3**

An analysis of the attacks that might be undertaken in each location-authentication setting.

(The colors indicate similarities between the schemes or settings.)

<table>
<thead>
<tr>
<th>Attack</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Distance fraud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Absolute-location fraud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Time fraud</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mafia fraud 0</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mafia fraud 1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Terrorist fraud 0</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Terrorist fraud 1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Device cloning</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Report manipulation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Signal and data manipulation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Signal and data synthesis</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Sybil attack</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Authorized licensed use limited to: Univ Carlos III. Downloaded on May 18, 2010 at 16:56:57 UTC from IEEE Xplore. Restrictions apply.
might try to make the reference nodes believe it’s at some location it actually left a while ago. In proximity-based schemes, the adversary might undertake this attack by trying to reuse previously received tokens at the target location.

In proximity-based schemes, tokens should be different each time.²⁰ Denning and MacDoran propose a similar mechanism to guarantee freshness and location authentication,⁹ while others rely on tamper resistance.¹⁵

**Mafia fraud**

In the classic version of this attack, adapted to location-authentication schemes (mafia fraud 0), the adversary places one or more malicious nodes T* (or R* in terminal-based schemes) acting as a proxy between honest reference nodes and an honest node T. The malicious node T* is placed at the target location l while T isn’t. The adversary’s goal is to make the reference or central nodes (the node T itself in terminal-based schemes) believe that T is at l. This attack is also called a wormhole attack.

When the target node interacts with a central node in addition to reference nodes, the mafia fraud attack can be made in a second way (mafia fraud 1). In this case, the malicious node T* is placed between the honest node T and the central node C. T is at the target location l while T* isn’t. The adversary’s goal now is to make the central node believe that T* is at l.

Avoiding this attack in round-trip-TOA-based schemes requires using signals propagating at a speed that the adversary can’t exceed (signals whose propagation speed is close to light speed).⁸,¹⁰,¹⁴

One way to mitigate the attack in proximity-based schemes is to control the access to the tokens by encrypting them with a key shared with the intended (honest) target node. Matthew Pirreti and his colleagues propose a similar mechanism that uses cluster keys shared only between the nodes close to the reference nodes.²² Other researchers suggest the careful design of reference-node deployment combined with specific requirements such as the use of rejector nodes or sectorized antennas.²¹ In another mechanism, the reference nodes use high-bandwidth signals or the target node performs noncryptographic validations to detect whether the signal has been relayed.¹⁵

**Terrorist fraud**

This set of attacks (terrorist fraud 0 and 1) is similar to mafia fraud attacks except that all participating nodes are malicious. So, the node that was honest in mafia fraud attacks now colludes with the other malicious nodes if there’s some authentication operation is involved.

To avoid this attack, the message that the target node sends must be bound to itself (using message authentication, for example) and its contents protected to avoid an adversary reusing them (such as through encryption).¹⁵

**Device cloning**

If the adversary controls and has cloned a compromised node, it’s easy to make reference or central nodes believe that the node exists at a fake location.

This attack is difficult to prevent, but tamper resistance and device-fingerprinting techniques can help.

**Report manipulation**

The infrastructure-based schemes that have the target node reporting information to a central node might suffer from this attack. The adversary might try to manipulate the report that an honest target node T sends to make the central node believe T is at an incorrect location.

Message authentication mechanisms can help prevent this attack.

**Signal and data synthesis**

An adversary might try to impersonate reference nodes to subvert location authentication protocols. This attack is easy to undertake using current public GPS signals.

To prevent this attack, a target node should be able to authenticate the signals received from reference nodes—or at least the data they carry.¹⁵

**Signal and data manipulation**

In satellite-based schemes, the signal’s ToA is very important. An attacker might manipulate the signals and the data they carry to selectively delay the signals’ ToA to an honest target node, which will therefore incorrectly estimate the target node’s location.

Message authentication mechanisms sometimes detect this kind of attack. However, satellite-based systems must include more specific mechanisms that can detect attacks that selectively delay the signal or manipulate its deviations.¹⁵,¹⁶

**Sybil attack**

In this attack, the adversary controls several compromised reference nodes R*, which collude to broadcast or send erroneous information to make the target node T determine T’s location incorrectly.

Once reference nodes have been compromised, target nodes can mitigate this attack using mechanisms that try to detect the fraudulent reference nodes to eliminate their influence in the location estimation.¹⁴,¹⁷,¹⁸

**Practical issues**

Analyzing how the proposed solutions mitigate the threats to location authentication is insufficient; we must also analyze the difficulty and cost of implementing the mechanisms in the context of a particular application to assess its suitability.

Generally, proximity-based schemes are more affordable and, if designed carefully, might stop an attacker that has reasonable capabilities. Other affordable and interesting schemes are those that don’t aim to prevent attacks at all cost but let the target node compute its location successfully with cer-
tain guarantees, given that the number of fraudulent nodes is limited.\textsuperscript{17,18}

The stronger schemes are usually more expensive to implement\textsuperscript{10,11,14,16} and might be adequate only for high-security applications. When analyzing the risk, you need to consider the adversaries’ resources and the differing contexts. For example, a weak adversary might be able to undertake attacks (for example, mafia fraud and signal synthesis attacks) in certain contexts but might require numerous resources to overcome other attacks.

Location authentication will receive increasing attention in ubiquitous computing. As we’ve learned, proposals designed for different contexts converge, and designing and implementing location-authentication mechanisms isn’t easy. On the one hand, range-dependent time-based mechanisms are generally more secure against powerful adversaries, but they usually impose hardware and software requirements that aren’t always easy to fulfill. On the other hand, robust statistical methods allow the provision of some guarantees to range-independent schemes without the strict hardware and software requirements. Although we focused on how the schemes address location authentication, we now must further study other parameters such as privacy guarantees, efficiency, hardware and synchronization requirements, and resilience to communication errors.

Several big challenges lie ahead for location-authentication researchers—mainly, building competitive commercial implementations of the mechanisms that can withstand attacks at an affordable cost. We must also develop formal methods for analyzing the mechanisms used to provide security guarantees.\textsuperscript{24} We’ll also need to integrate the authentication of a user’s proximity to the located devices to improve the integrity of existing or new mechanisms used in this field.

**Acknowledgments**

The authors are funded by a research grant of the Research General Directory from the Ministry of Education and Science in Spain under contract SEG2004-02604.

**References**


