W-SPS: Designing a Wide-Area Secure Positioning System

***Abstract*—Motivated by the security and functional limitations of satellite positioning systems, we explore a design of a Wide-Area Secure Positioning System. The main goals of this system are strong spoofing resilience, location verification, and privacy. We propose a realization of a Wide-Area Secure Positioning System and show that this solution is viable and can fulfill our defined security goals. Specifically, our system is composed of a secure positioning infrastructure to obtain reliable location information of an entity and a location verification architecture that allows others to be convinced of certain location properties of such an entity. The proposed system enables the verification of location claims in a privacy-preserving manner, thus enhancing existing security solutions and supporting future location-based applications.**

I. Introduction

Satellite navigation systems [1]–[3] have been exceptionally successful and are used today in numerous applications. In addition to vehicle navigation, these systems are used for synchronization of devices in distributed infrastructures [4], [5], tracking of people and valuables [6], toll collection [7], navigation of drones, etc. Therefore, security and safety critical applications are increasingly relying on satellite positioning systems to provide trustworthy input. With the expected wider deployment of autonomous systems such as self-driving vehicles [8], drones [9] and more generally of cyber-physical systems [10] and Internet of Things [11], the reliance on location and time information will only increase.

Recent practical spoofing attacks [12]–[16], fueled by the increasing availability of satellite signal generators[1] demonstrate that these systems currently do not provide strong security guarantees. Years of research into securing these systems further show that there are no simple fixes to this problem and systems remain vulnerable to dedicated adversaries. This is a fundamental limitation of the design of satellite positioning systems that cannot be fixed by a simple upgrade. Reliance on broadcast communication allows these systems to scale; however, they are inherently vulnerable to spoofing by attackers that control the communication channel and are capable of delaying, relaying, or generating navigation messages [17], [18]. This problem persists even if navigation messages are cryptographically protected.

Beside the inability to fully counter spoofing attacks, satellite positioning systems have another limitation — the infrastructure cannot verify the (claimed) location of a device since it is the device that, based on the received signals, computes its location. The ability to verify claimed locations of devices is clearly relevant in all scenarios where location is used in decision-making and where entities cannot be trusted to report correct locations. Examples of research proposals and real-world deployments that rely on location verification are numerous and include tracking of untrusted entities (e.g., offender ankle bracelets) [19], location-based access to services [20], confinement of traffic within a particular geographic area, etc. The distance of the satellites results in weak signals on the ground, making satellite positioning systems vulnerable to jamming [21] and spoofing attacks. It also limits the use of such systems in indoor environments. Legacy navigation systems (such as LORAN [22]) that were used prior to the deployment of satellite systems equally rely on broadcasts from ground stations and thus suffer from a number of the same limitations as satellite positioning systems[2].

We argue that the limitations of the existing positioning systems call for the development of a new, *wide-area* secure positioning system that provides security and functional guarantees that they lack, namely, strong spoofing resilience and location verification. This new system not only needs to provide an enhanced way by which positions are measured and calculated in order to counter (largely physical-layer) attacks, it also needs new global components that allow remote entities to encode and verify each others' locations.

In this work, we propose such a system that we call *Wide-Area Secure Positioning System (W-SPS)*. Our system combines two main components (i) the *Secure Positioning Infrastructure*, which issues verifiable location statements, and (ii) the global *Location Name Service*, which enables entities to map locations to labels and verify location statements corresponding to those labels. The Secure Positioning Infrastructure (SPI) primarily consists of stations, deployed within the target coverage area (city, country), that are used to calculate verifiable device locations. Unlike satellite positioning systems, different SPIs (covering distinct or overlapping areas) can be developed and deployed independently, be controlled by local authorities (e.g., countries), and issue location statements that are globally verifiable and pertain to the area that they control[3]. For example, a Norwegian SPI

[1]GPS signal generators with advanced features such as record and replay, generating signals for a static location and time or for a dynamic route are available for under $7000. Home-brew spoofers can be realized based on software-defined radio platforms that cost less than $1500.

[2]Even if LORAN was largely decommissioned over the last decades, there is recently a renewed interest in its use in scenarios where satellite systems are subject to jamming attacks [21].

[3]In recent years, several countries, including France, Japan, and India, are investing in regional navigation satellite systems.

can issue a signed statement that a specific device has proven to be in the vicinity of Kirsten Flagstads Plass 1, 0150 Oslo, Norway on Jan 2, 2014 at 14.15h; such statements can be issued at different levels of time and location granularities and be bound to different device identifiers. Statements from local SPIs can only be meaningful if the locations contained in their statements are geographical coordinates or can be mapped to geographical coordinates by the verifiers. Public government databases can be trusted to map administrative divisions to geographic coordinates, but do not map user-generated labels (e.g., businesses) to coordinates. A Location Name Service (LNS) fills this gap and provides a way for the users to obtain a trusted mapping between common names (e.g., "Universitetet i Oslo") and geographic coordinates.

There are many possible realizations of a Wide-Area Secure Positioning System providing different security and privacy guarantees. Realizations of W-SPS based on existing systems such as cellular positioning and online maps [23], [24] could increase the difficulty of an attack, but would still be ineffective against dedicated adversaries. We therefore propose a realization of a W-SPS that is spoofing resilient, supports location verification and remote verification of location statements. The main component of our system is a new Location Name Service, which provides trustworthy mappings between labels and their associated locations, and a set of associated protocols which allow devices to prove their locations to third parties in a privacy-preserving manner. Our Secure Positioning Infrastructure builds on previously proposed location verification protocols using distance bounding, and therefore allow a set of infrastructure nodes to verify location claims of devices (i.e., perform location verification). Here we show that such location verification protocols can be deployed in wide-areas and we discuss challenges related to this deployment.

In summary, we make the following contributions. (i) We argue the need for a novel, wide-area secure positioning system. (ii) We define the main functions of this new system and propose the components that implement these functions. (iii) We propose and evaluate a concrete realization of a wide-area secure positioning system.

We see this work as a first step towards opening a discussion about the design of a new secure positioning system, properties that it should have and applications that it should support.

II. Background and Problem Statement

In this section we review the security of existing positioning systems and motivate the need for a new secure positioning and location verification system.

A. Security of Positioning Systems

Positioning services are typically used for navigation and tracking. In a navigation scenario, an infrastructure (e.g., GPS) typically broadcasts signals that a device uses to compute its location. In a tracking scenario, it is often the device that transmits beacon messages to allow the infrastructure to compute its location e.g., using Time-Difference-of-Arrival (TDoA) [25]. In non-adversarial settings, systems used for navigation can be used for tracking since we can trust the device to report the true calculated location to the infrastructure. Equally, if we know that the positioning is not influenced (i.e., spoofed) by the attacker, we can trust that the position that is computed by the infrastructure or by the device is actually correct (within a positioning error).

In adversarial settings, however, these assumptions are no longer valid. Navigation systems, such as GPS, operate by broadcasting signals from the satellites. It is the differences of the times of arrival of the signals from different satellites at the receiver that actually determine the position that the receiver calculates. An attacker that is able to change the arrival times of the signals at the receiver can therefore modify (spoof) the calculated position. Such attacks have been shown to be feasible both in theory and practice [12]–[16]. Terrestrial navigation systems such as LORAN-C, DELTA and OMEGA [26] have similar drawbacks. TDoA-based tracking systems are also vulnerable to spoofing by attackers capable of selectively delaying signals from the devices to the infrastructure. Spoofing detection mechanisms can be built by leveraging redundant positioning systems, such as inertial navigation systems, the use of online maps, WiFi, cellular networks and GPS [27]. These approaches are, however, application-specific, require calibration and need to account for WiFi and cellular network spoofing [28]. A number of works have studied how to increase spoofing resilience of GPS receivers, leveraging spatial diversity, noise level detection, presence of vestigial signal, and enabling integrity through delayed key disclosure [29]–[33]. However, although these approaches increase resilience to spoofing, they fail to prevent it in all contexts. Spoofing remains especially difficult to prevent if the attacker is in the close proximity of the victim device. Deployed positioning systems therefore do not provide strong spoofing resilience.

If the localized device is untrusted, it cannot be trusted with reporting a correct location. In the case of GPS, a device can simply report an incorrect location. This problem cannot be solved by the deployment of trusted computing since the attacker can spoof the signals that are received by the trusted module and therefore spoof the calculated location. In the case of TDoA-based tracking systems, an attacker can use directional transmissions to selectively deliver signals to infrastructure nodes, effectively cheating on its own position [34].

As a response to these limitations, a number of new positioning systems have been proposed [18], [35]–[38]. Verifiable multilateration [18] provides provable protection against spoofing attacks, and supports location verification. It relies on distance bounding radios, for which research and commercial prototypes have started to emerge [39], [40].

Given the properties that it provides, we evaluate the use of verifiable multilateration for location verification in our Secure Positioning Infrastructure (Section IV).

B. Problem Statement

We motivate the need for a new secure positioning system through an abstract example. In our example, two parties communicate online, and prior to starting the communication they want to prove to each other that the communication will take place from within approved locations. During this process, they want to preserve the privacy of their exact locations. For example, the *verifier* wants to establish that he is talking with an employee (the *prover*) of a certain company only while he is at the company premises. The company can have offices globally and the prover wants to convince the verifier that he is in one of those offices without disclosing in which one.

Supporting this verification requires several functions to be in place. This includes (i) a (secure) mechanism to compute the prover's location, (ii) the ability to issue and verify global location statements bound to an identity and (iii) a trusted public database that contains the locations of the company offices.

We note that in this example, the complexity of the verification and of the trust assumptions that need to be made stems from the fact that the list of locations of company offices is not common public knowledge and thus requires both certification and verification. If, for example, the prover wanted to convince the verifier that it is in a particular city (e.g., Oslo, Norway), it is sufficient for the secure positioning infrastructure of Oslo to verify the prover's location and issue a signed statement indicating that the prover is indeed in Oslo. This example shows how location verification for common administrative and geographical labels ("Oslo") differs from the verification process that is required for user-generated location labels ("Company").

An example of a concrete use of secure location verification is online banking. Here, the bank client (the verifier) wishes to be certain, before it performs any transactions, that it is communicating with the bank servers (the prover) that are located at "proper" locations (e.g., in his country of residence). Another example is the one of modern drones or quadcopters which are gaining popularity [9]. If drones are compromised (e.g., due to a software vulnerability), they might change course or perform unexpected maneuvering. Being able to verify their locations will provide another way of detecting anomalous behavior and thus detecting their compromise. In this example, however, privacy issues might be secondary. These examples are only representative of a number of current and future scenarios where location verification can support security functions. Motivated by them, we state our problem as follows.

Problem Statement. We consider a *prover* whose goal is to convince a remote *verifier* of its presence at one of many locations from a given location set. Our goal is to design a W-SPS that enables this verification and provides the following main guarantees.

- *Positioning Security.* Positioning must be spoofing-resilient.
- *Verification Security.* The prover must not be able to prove that it is present at one of the locations from the set unless it is really located at one of those locations.
- *Privacy of the prover's identity.* The prover needs to be able to preserve the privacy of its identity with respect to the W-SPS.
- *Privacy of the prover's location.* The prover needs to be able to preserve the privacy of its location with respect to the verifier and even with respect to the parts of the W-SPS infrastructure in that it can choose to disclose its location with some degree of certainty and granularity.

Here, when analyzing spoofing resilience, we consider an external attacker whose aim is to influence the location computation process. When analyzing location verification, we further assume that the prover is untrusted and has an incentive to violate this security property to deceive the verifier about its location. When analyzing privacy, we assume that the verifier wants to violate the prover's privacy by learning its location. We finally assume that the W-SPS is honest-but-curious both about prover's location and identity. We explicitly exclude denial-of-service attacks.

III. Solution Overview

Our W-SPS is designed to be deployed over a wide geographical region that is divided into multiple *administrative domains* (AD). Administrative domains could be standardized, e.g., using ISO-3166 [41]. Furthermore, a user could define his own domain, referred to as a *user-defined domain* that spans multiple non-contiguous regions across different administrative domains. For example, a multinational corporation (the user in this case) may define its own domain that corresponds to its office locations across different countries (the ADs).

Our W-SPS relies on two components: a *secure positioning infrastructure* (SPI) and a *location name service* (LNS). Each administrative domain can have its own independent SPI that provides secure positioning services within each domain. For example, an SPI could be maintained by a local government or a telecommunication provider in the country (an AD in this case).

The SPI consists of multiple wireless base stations installed across an administrative domain. A prover requests the SPI to compute its location and issue a *signed location statement*. This statement contains the prover's identity and location information at a given time. For example, a signed location statement could contain information in different granularities, e.g., the country, city, or even geometric coordinates of the prover.

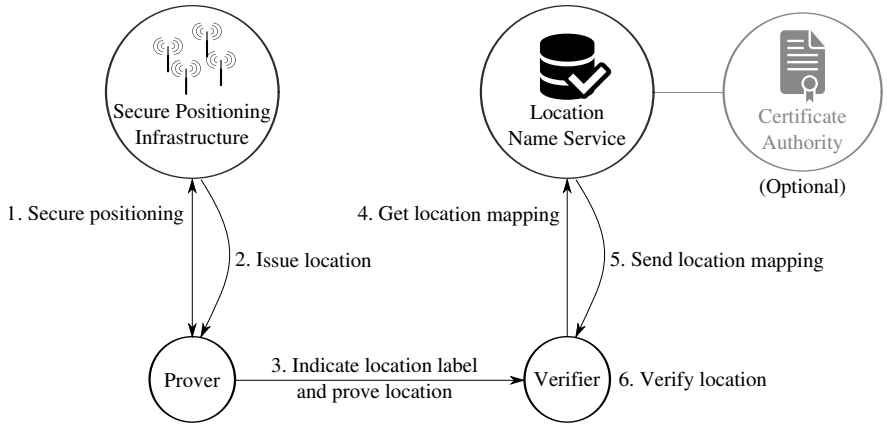

Figure 1. System overview. The location name service stores a database mapping a location label to a set of locations during a registration process, which is later provided to the verifier on request. The prover and the secure positioning infrastructure perform secure positioning, after which the infrastructure issues a signed location statement to the prover. The prover uses the location statement to prove its presence in one of the associated locations the verifier downloads from the location name service. A CA is optionally involved to certify an identity during the location mapping registration process if it is included in the label.

In order to support privacy-preserving location statements across different administrative domains, we propose the use of a location name service. The LNS is a trusted store containing signed entries that map user-defined labels (referred to as *location labels* to their corresponding sets of locations). The locations are defined by SPIs under one or more administrative domains, e.g., as defined in ISO-3166. The entries are added via a registration process. The signature of each entry is generated during this process by the registrant, and is used during the location verification process. The entry also contains the public key used to verify its signature. The LNS allows user to create custom anonymity sets beyond administrative borders and use them for privacy-preserving location verification.

Verifying the Prover's Location. We now provide a high-level description how W-SPS is used for location verification, shown in Figure 1. Note that all communication channels are assumed to be secure, i.e., confidential and authentic. We assume that the location name service already contains the mapping required for the location verification process, which consists of the following steps.

1) The secure positioning infrastructure localizes the prover using verifiable multilateration and distance bounding. Details of this process and its real-world feasibility are explored in Section IV. After obtaining the prover's location, the infrastructure issues a signed location statement that contains the prover's identity, location information, and a timestamp.
2) The verifier obtains the location label that is to be used to verify the prover's location. This can either be obtained from the prover or known beforehand. First, the verifier queries the LNS with this location label to obtain the corresponding entry. Then, the verifier ascertains that the public key contained in the entry belongs to an entity that it trusts. Finally, it verifies the signature in the entry before accepting it.
3) The prover uses the signed location statement to convince the verifier that it is present at one of the locations associated with its location label.

In the following sections, we discuss the secure positioning infrastructure and the protocols used by the prover and verifier to achieve privacy-preserving location verification in detail.

IV. Secure Positioning Infrastructure (SPI)

The secure positioning infrastructure (SPI) is responsible for issuing a location statement containing a prover's location that can be globally verified. In order to accomplish this task, the SPI needs to compute or verify the prover's location securely. Specifically, an attacker (e.g., an external MiTM attacker or a malicious prover itself) should not be able to influence the position computed by the SPI either by delaying, relaying, replaying or generating messages. As described in Section II, existing positioning and ranging techniques are vulnerable to such attacks. This motivates the need to design and implement a novel positioning infrastructure. In this section, we describe the design of such an infrastructure which we refer to as the Secure Positioning Infrastructure and discuss its design choices.

A. Overview

Our SPI consists of base stations capable of executing distance bounding protocols with a prover whose location needs to be securely determined and verified. These base stations are deployed across a wide geographic area of interest at various altitudes from the ground level as shown in Figure 2. For example, they can be fixed on top of buildings, similar to cellular network base stations, or at the ground

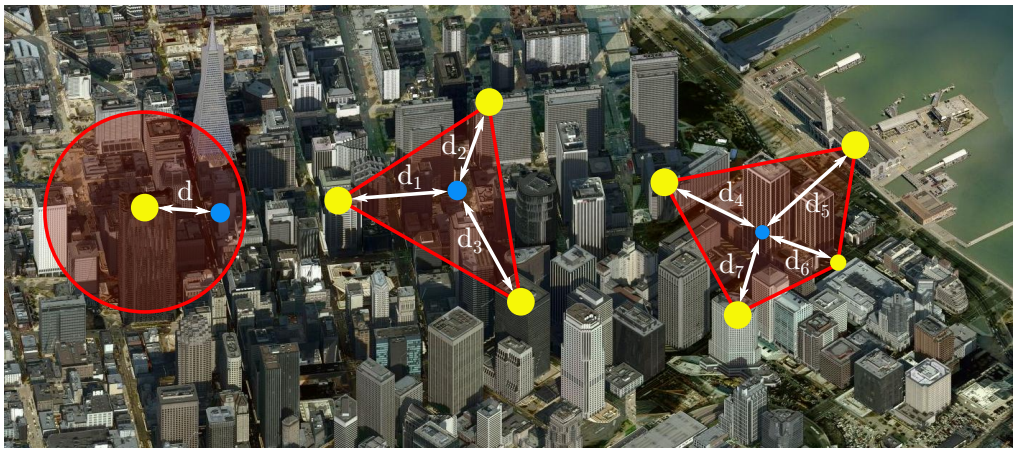

Figure 2. Example deployment of base stations in a typical urban environment showing deployment over roof tops as well as ground-level. Three different scenarios where the prover is in the coverage region of one, three and four base stations is illustrated.

level, similar to wireless access points. Optionally, for better precision and stronger security guarantees, some of the base stations can be mobile.

In order to securely compute the position of the prover, a set of base stations execute distance bounding protocols with the prover to estimate their mutual distances. Based on these estimated distances, the SPI derives the prover's position using verifiable multilateration and issues a location statement that can be globally verified (details in Section V). For certain applications, it might be sufficient to position the prover with coarse granularity (e.g., city or district). In such scenarios, the prover can simply execute distance bounding protocol with one of the base stations. Since distance bounding inherently confirms proximity, the infrastructure can then issue a location statement indicating the prover's proximity to that specific base station (Figure 2).

In this section, we briefly describe the concepts of distance bounding and verifiable multilateration and how we use them to realize our secure positioning infrastructure. In addition, we explain our choice of physical layer and evaluate its feasibility of deployment in typical urban environment.

B. Distance Bounding and Verifiable Multilateration

Distance bounding protocols were first introduced for wired systems by Brands and Chaum [42]. The goal of distance bounding is that a verifier establishes an upper bound on its physical distance to a prover, i.e., an external attacker or a malicious prover cannot claim to be closer to the verifier than its actual distance. Distance bounding protocols [36], [43]–[50] follow a specific procedure which typically includes a set-up, rapid bit exchange and verification phase. In the set-up phase, the verifier and the prover agree or commit to specific information that will be used in the next protocol phases. In the rapid bit exchange phase, the verifier challenges the prover with a number of single-bit challenges to which the prover replies with single-bit responses. The verifier measures the round-trip times of these challenge-response pairs in order to estimate its distance to the prover. The distance d between the verifier and the prover is calculated using the equation $d = \frac{c \cdot (\tau - t_p)}{2}$, where c is the speed of light ($3 \cdot 10^8$ m/s), τ is the measured round-trip time and t_p is the processing delay at the prover before responding to the challenge. The verification phase is used for confirmation and authentication.

Verifiable multilateration [18] leverages both multilateration and distance bounding to securely (verify) compute the prover's (claimed) position within a region encompassed by a set of reference nodes. Verifiable multilateration can be explained in the following steps:

1) Three (or more) verifiers form a verification triangle (polygon).
2) Each of the verifiers estimate its distance to the prover using distance bounding.
3) Based on multilateration technique, the verifiers then compute the prover's location.
4) If the computed location is within the verification triangle (polygon), one can conclude that the prover's claimed location is correct.

For example, consider the prover within the coverage area of three base stations (Figure 2). In order to be spoofed or to claim a false position within the verification triangle formed by the base stations, the attacker needs to reduce the distance to at least one of the base stations. This is not possible since distance reduction attacks are inherently prevented by distance bounding.

C. Deployment Feasibility

Choice of Physical Layer: In distance bounding, the precision of the measured distance depends on the accuracy with which the round trip time is estimated. For example, a 1 μs error in estimation results in a distance measurement error of 300 m. Accurate measurement of arrival time is

dependent on the physical properties of the transmitted information (e.g., symbol duration, type of modulation scheme used). In addition, the success of distance reduction attacks such as early-detect and late-commit [51], [52] depend on the physical-layer characteristics. Thus, the physical layer plays an important role in the security and performance of the system.

As explained in Section II, ranging systems based on received signal strength and ultrasound are inherently insecure. For example, an attacker can fake the signal strength in an RSS-based distance measurement system. Similarly, in an ultrasonic ranging system, an attacker can gain advantage by relaying messages over the faster radio frequency channel [53]. In addition, the precision of a ranging system depends on the bandwidth of the signal used for ranging. The higher the bandwidth, the better is the precision. For short and medium-distance precision ranging and localization, ultra-wide band (UWB) and chirp spread spectrum (CSS) are commonly-used techniques and are standardized in IEEE 802.15.4a [54] and ISO/IEC 24730-5 [55]. Distance ranging with CSS-based systems relies on time-of-flight (TOF) measurements obtained by accurate time-of-arrival (TOA) estimation of chirp signals. Chirps are sinusoidal signals whose frequency varies with time. Chirp signals [56] have been extensively used in radar and sonar systems [57], [58]. Although the properties of CSS [56], [59] allow low-complexity and low-power implementations of both the transmitter and receiver on a single integrated hardware [60], their existing implementations are vulnerable to physical layer attacks [61].

Ultrawideband impulse radio (UWB-IR) ranging systems use extremely short pulses which are typically $2-3\,\mathrm{ns}$ long. Range estimation is based on the time elapsed between transmitting a challenge pulse and receiving a corresponding response. Due to the use of extremely short pulses (i.e., large signal bandwidth), IR-UWB ranging systems have high precision (within a few centimeters) and are resilient to multipath effects that are predominant in an urban environment. The security properties of UWB-IR based ranging systems have been thoroughly analyzed in [62], [63].

In summary, the ranging resolution, reliability and robustness to multipath channel effects make UWB-IR and CSS favorable candidates for the physical layer. In addition, the increasing number of commercially available ranging systems [64]–[67] helps in evaluating their security and performance in a typical urban environment.

***Communication Range**:* The communication range depends on the choice of physical layer, receiver sensitivities, transmission power and signal path loss[4]. Figure 3 shows the simulated path loss in both free space (line-of-sight) and log-normal fading models for an UWB signal centered at $5\,\mathrm{GHz}$. The log-normal fading model is an extension of the free space propagation model but also takes into account the slow and fast fading effects due to multipath components. We observe that at a distance of $200\,\mathrm{m}$ the signal is attenuated by at least $100\,\mathrm{dBm}$. Existing commercial UWB-IR ranging systems [64]–[67] are capable of receiving signals with power levels up to $-110\,\mathrm{dBm}$. Thus we can safely assume a communication range of $\approx 200\,\mathrm{m}$ (assuming FCC's maximum specified power limit of $0\,\mathrm{dBm}$ for UWB [54]) for a base station. We note that the above estimated range is limited due to the FCC limits and can be further improved by increasing the transmission power levels and the base station receiver sensitivities.

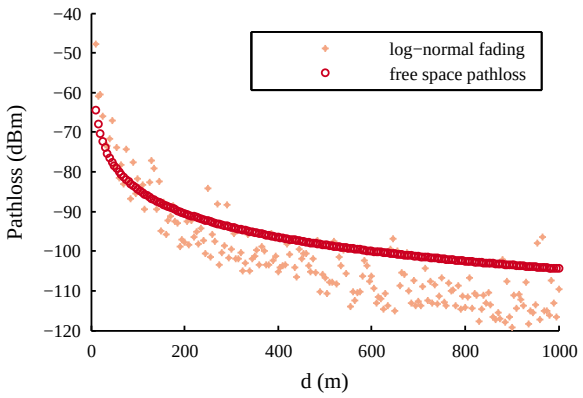

Figure 3. Simulated path loss based on both the free space propagation model and the log normal fading model. It is observed that the signal strength attenuated to about $100\,\mathrm{dBm}$ at a distance of $200\,\mathrm{m}$.

***Coverage**:* Based on the calculated communication range, we now determine the number of base stations required to realize our secure positioning infrastructure over a wide area. The number of base stations depends on the granularity required by specific applications. For example, it might be sufficient to estimate a location with coarse granularity (e.g., city or a zone in a city) for certain applications while others might require more precise position estimates. For coarse-grained position estimates, the prover needs to be within the coverage area of just one or two base stations. Thus, for such applications, it is sufficient to have a base station every $400\,\mathrm{m}$ (assuming a base station range of $200\,\mathrm{m}$). For higher precision positioning estimates, the prover needs to be within the coverage area of four or more base stations (Figure 2). The intuitive way is to position the base stations at the vertex of an inverted triangular pyramid, as shown in Figure 4. Note that each of the base stations must be at most R units away from each other, where R is the base station communication range that restricts the maximum height of the pyramid. The maximum height of the pyramid should not exceed $\frac{\sqrt{3}\cdot R}{2}$ for total coverage within the verification pyramid. The minimum number of base stations N required for complete coverage of an area

[4]The loss in signal strength experienced by the signal as it propagates through the environment.

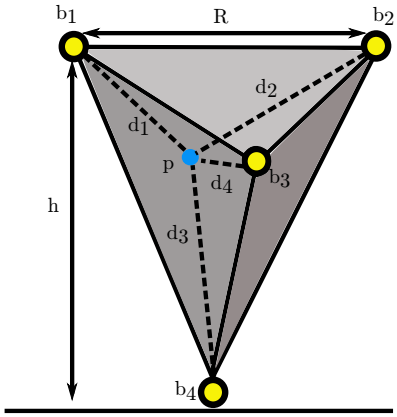

Figure 4. Coverage of verifiable multilateration using four base stations

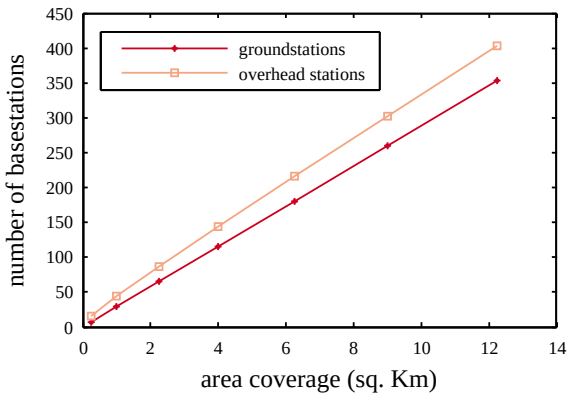

Figure 5. Number of overhead and ground basestations required to cover a certain area.

$L \times L$ up to a height h is given by the following equation:

$$N = \frac{(\frac{2L}{R} + 3) \cdot (\frac{L}{h} + 1)}{2} + (\frac{L}{R}) \cdot (\frac{L}{h}) \quad (1)$$

Figure 5 shows the total number of base stations required for covering a specific area given a base station communication range of $R = 200\,\mathrm{m}$. We observe that in order to cover an area of 2 square kilometers, we need a total of 100 base stations for complete coverage. In contrast to conventional communication systems, constant connectivity is not a requirement in our secure positioning infrastructure. In the majority of application scenarios, it is sufficient for the base stations to communicate with the prover only for the duration of execution of distance bounding protocols. Thus, one can also use mobile base stations (e.g., mounted on trams and buses with known routes) to improve coverage. In addition, the use of mobile base stations can improves the precision of the estimated position as proposed in [68].

Performance: We now provide a conservative estimate of the time taken to compute or verify the position of a prover. For distances up to $200\,\mathrm{m}$, existing UWB ranging systems [64]–[67] take up to $200\,\mathrm{ms}$ to perform one ranging operation. As explained previously, for applications that require precision position estimates, it is necessary to execute at least four such operations. In addition, the secure positioning infrastructure needs to execute the initiation and final verification phases of the distance bounding protocol.

D. Discussion

Verifiable multilateration faces the threat of cloning attacks. An attacker, after gaining access to multiple provers, can use the same identity across all provers and strategically places them within the verification region next to each of the base station. This allows the attacker to convince the infrastructure that it is at any position within the verification region. Such attacks can be prevented by the use of trusted computing platforms that provide tamper resistance. However, the trusted computing platform alone does not prevent an attacker spoofing the signals received by the trusted module.

In our design, an attacker can collude with a dishonest prover to force the secure positioning infrastructure to compute a false location. Such attacks is referred to as terrorist fraud attacks. A number of protocols have been proposed to prevent terrorist fraud attacks [44], [69]. The majority of these protocols use symmetric cryptography, thus requiring the prover and the infrastructure to share credentials beforehand. However, it is possible to leverage the protocol proposed in [70] to prevent terrorist fraud attacks in our infrastructure without using shared keys.

V. Location Verification Protocols

A trivial solution to location verification involves the prover obtaining a signed location statement containing its identity and location information from the secure positioning infrastructure and forwarding it directly to the verifier. This solution, however, does not preserve the privacy of the prover since the infrastructure learns its identity and the verifier learns its true location. In order to overcome these limitations, our design instead uses anonymous credentials and signature schemes proposed by Camenisch and Lysyanskaya [71], [72] to achieve the same goals without compromising the prover's privacy.

In the following, we first describe the adaptation of anonymous credentials for location verification. We then outline the protocols used by the W-SPS, the prover, and the verifier to achieve location verification.

A. Anonymous Credentials

We use anonymous credentials [71] and the Camenisch-Lysyanskaya (CL) signature scheme. We refer the reader to the original proposal for further details [72].

Generating keys: In the generalized CL signature scheme for multiple messages, the public key is a tuple $(n, a_1, ..., a_N, b, c)$, consisting of (i) a special RSA modulus $n = pq$, where p and q are safe primes, and (ii)

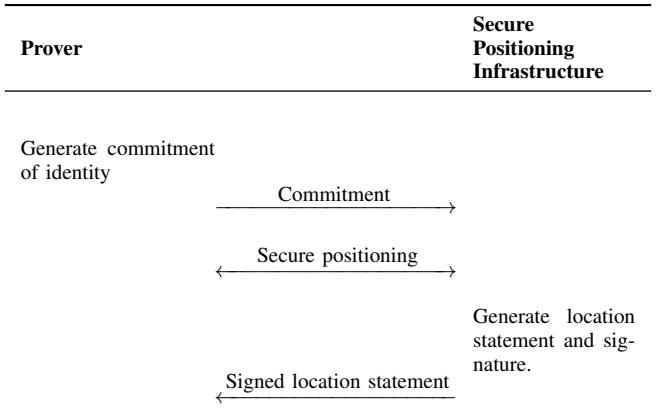

Figure 6. Obtaining a signed location statement. The prover sends a commitment of its identity and engages in secure positioning. The secure positioning infrastructure obtains the location and generates a signed location statement that is issued to the prover. The commitment of the prover identity preserves the privacy of the prover.

$a_1, ..., a_N, b, c \in QR_n$, generators that are distinct quadratic residues modulo n. The corresponding secret key is p, one of the prime factors of n. N is the number of message blocks (in this case, the number of data fields) to sign. The data fields include the prover's identity, the time, and the different fields of the location data.

Signing and verifying: The signature on the message blocks $m_1, ..., m_N$ is of the form (e, s, v). Here, e is a random prime and s is a random number generated by the signer. The value v is computed as $v = (a_1^{m_1}...a_N^{m_N} b^s c)^{1/e} (\text{mod } n)$. The signature can be verified by checking if $v^e = a_1^{m_1}...a_N^{m_N} b^s c \ (\text{mod } n)$ holds.

Blind signing: The CL signature scheme also allows a signer to generate signatures on unknown messages. An entity requesting a signature on a secret message block m_i can blind m_i by sending the signer the value $C_i = a_i^{m_i} b^{s'}$, where s' is a random number. The signer generates a random prime e and a random number s, and computes $v = (C_i a_1^{m_1}...a_{i-1}^{m_{i-1}} a_{i+1}^{m_{i+1}}...a_N^{m_N} b^s c)^{1/e} \text{ mod } n$ to produce the signature (e, s, v). The signature for the message blocks is $(e, s+s', v)$. This mechanism is later used to preserve the privacy of the prover's identity from the secure positioning infrastructure.

Zero-knowledge signature proof: The CL signature scheme allows zero-knowledge proofs of a valid signature on a message. Additionally, it also allows the proof of certain properties (e.g., inequalities) of the message itself. In these proofs, the verifier learns neither the hidden message contents nor the signature.

B. Obtaining the Signed Location Statement

The secure positioning infrastructure generates signed location statements. Each statement contains (i) the identity (e.g., public key) of the prover, (ii) the timestamp when the infrastructure calculates the prover's location, (iii) location data, and (iv) the signature. Note that the SPI does not learn the prover's identity because the request for the statement only contains the blinded identity. Location data could be of various forms, such as country, county, city, or even geographic coordinates. The CL signature scheme is used to sign these data fields. Each individual piece of information is associated with its own quadratic residue generator during signature generation.

The process of obtaining the location statement is illustrated in Figure 6. The commitment is the blinded value of the prover's identity, and is sent to the secure positioning infrastructure. On receiving this, the infrastructure performs secure positioning to obtain the location of the prover. The infrastructure then signs a location statement consisting of the committed value, a timestamp, and the location; it then sends the resulting signature to the prover together with the location and timestamp.

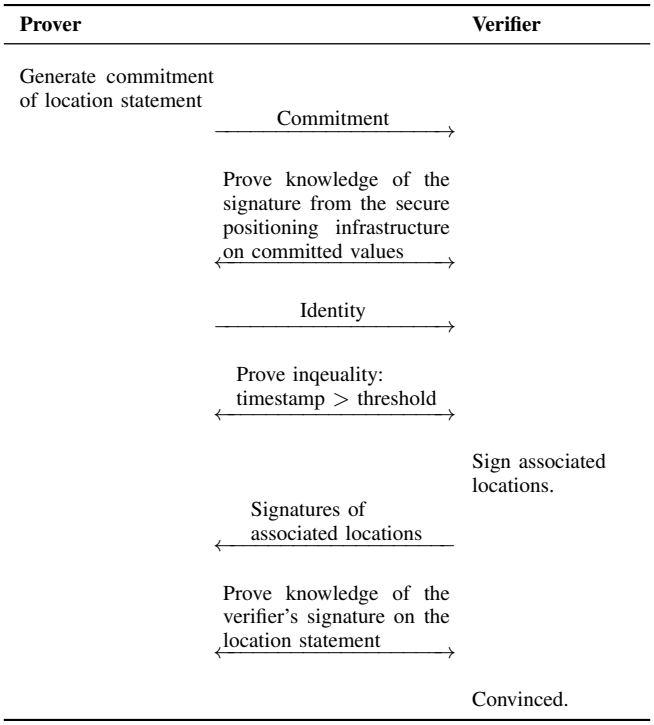

Figure 7. Privacy-preserving location proof. For simplicity, we assume that the verifier already has the location mapping containing the location label and the associated locations. The proof consists of two main parts: the first part proves the knowledge of a valid signature from the secure positioning infrastructure; the second part proves the membership of the location in the set of associated locations.

C. Proving Location Correctness

In certain scenarios where the privacy from the verifier is not required, the prover may directly present the signed location statement to the verifier.

However, to achieve location privacy, we use a two-phase process involving zero-knowledge proofs and set membership proofs. First, the prover users a zero-knowledge proof

Table I
OVERHEAD OF LOCATION ISSUANCE AND VERIFICATION

Operation	Computation Time (ms)	
	Median	Std. deviation
Signed location statement issuance	313.9	135.4
Associated location signature issuance	13829.5	958.9
Proof generation	211.1	4.7
Proof verification	156.0	4.9

of knowledge to convince the verifier that it has a signed location statement. Next, the prover establishes the validity of its location using set membership proofs.

The complete protocol is shown in Figure 7 and consists of the following steps:

1) The prover sends the verifier a commitment of all the location data values in the signed location statement.
2) The prover uses a zero-knowledge proof to convince the verifier that it has a valid signed location statement. The prover also reveals the corresponding identity in the location statement.
3) The prover uses a zero-knowledge proof to assure the verifier that the timestamp is fresh.
4) The verifier signs the set of locations associated with the location label and sends the signatures to the prover.
5) The prover uses another zero-knowledge proof to demonstrate that it possess a signature from the verifier on its location statement. If the prover cheats by using a signed statement corresponding to a location different from the ones associated with the location label, it would not have a valid signature from the verifier [73].

D. Security Analysis

We analyze our architecture with respect to the security and privacy properties defined in Section II-B.

The external attacker cannot influence the location computation process performed by the secure positioning infrastructure as discussed in Section IV. Also, the external attacker cannot influence any communication between the prover, the verifier, and the W-SPS because it occurs over secure channels.

Similarly, an untrusted prover can neither influence the communication channel between the verifier and the LNS nor cheat during the location computation process of the secure positioning infrastructure. Moreover, the prover cannot subvert the location verification protocol to mislead the verifier into believing that it is at a false location due the CL signature scheme and its accompanying zero-knowledge proofs [72], [73]. Hence our W-SPS ensures that the prover cannot cheat on its location.

Our design also guarantees the privacy of the prover's identity from a curious W-SPS. This is achieved using the hiding property of the blinding signing process in CL signatures [72]. The prover's location privacy against a curious verifier is also guaranteed by the zero-knowledge property of the proofs.

Table II
CONTENTS OF LOCATION STATEMENT

Category	Data type
Identification	Prover identity
Timestamp	Time since defined epoch
Geopolitical	Country First-level division (e.g., state) Second-level division (e.g., county) Third-level division (e.g., city) Forth-level division (e.g., municipality) Postal address
Geometric Coordinate	Coordinates with granularity level 1 ... Coordinates with granularity level N_g

E. Implementation and Evaluation

We implement the protocols described in Section V-C using idemix [74] to evaluate their performance. We optimized the implementation by combining the proofs and converting the protocol to a non-interactive zero-knowledge proof using the Fiat-Shamir heuristic [75].

Table II lists the different location information used in our implementation to realize the location statement. They are explained as follows.

Due to the different administrative divisions in different countries, we adopt the ISO-3166 standard for a unified location format in the signed location statement [41]. In this standard suite, the geopolitical location information consists of the fields shown in Table II. A location statement also consists of different sets of geometric coordinates, each corresponding to a particular granularity. A granularity level refers to the level of precision in terms of the prover's longitude, latitude, and elevation. We denote the number of different granularities of the prover's location in the location statement by N_g; the location statement therefore contains N_g sets of geometric coordinates.

Evaluation: In order to reflect real-world constraints, we also adopt security parameters that are similar to those used by Bichsel et al. [76] for smart cards implementing the Java Card. Specifically, the modulus n is 1536 bits long, the generators a_i, b, c are each 1536 bits long, and each signed message block is 593 bits long. We also set N_g to be 5. In the evaluation, we consider a set of 50 locations associated one location label. Each location is represented by the geometric coordinates in the highest granularity (10^{-4} degrees for longitude and latitude, and 10 meters for elevation). We run the protocols on a ThinkPad T420 running an Intel Core i7 CPU clocked at 2.7 GHz for 1000 iterations.

The results are shown in Table I. Runtime Profiling

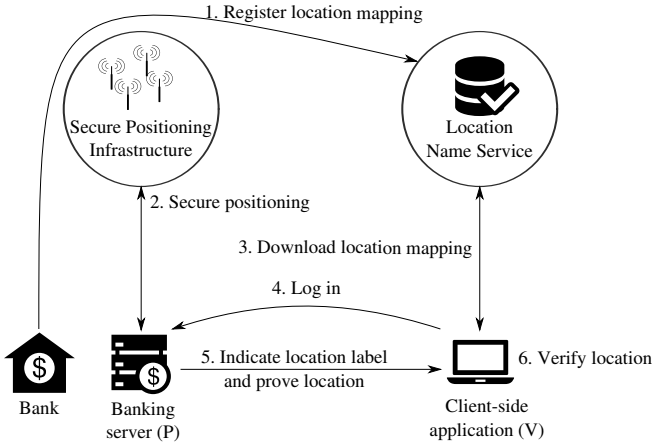

Figure 8. Example realization of the architecture in the online banking scenario. The location mapping is registered by the bank to location name service. The prover is the bank server and the verifier is the client-side application of the user.

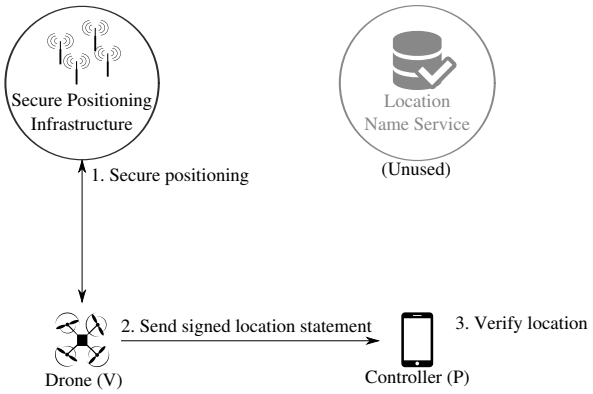

Figure 9. Example realization of the architecture in a drone tracking scenario. The secure positioning infrastructure regularly positions the drone and issues signed location statements. The statements are forwarded by the drone to its controller.

using jvmmonitor [77] indicates that the primary source of variance in the computation overhead in the first two procedures is due to the iterative process of generating their respective random prime number e in the CL signature scheme. Evaluation shows that signing of the locations by the verifier is the most computationally intensive of the entire protocol. However, this can be optimized by having the verifier precompute the signatures.

In terms of storage overhead, the size of the signed location statement containing the information as shown in Table II is approximately 6.2 KB; the size of a single location signature is approximately 2.2 KB.

VI. Applications

We illustrate the use of W-SPS using two possible example scenarios. We assume that the location name service is realized as a trusted server set up by an authoritative entity. The secure positioning infrastructure is implemented by a local telecommunication service provider.

Online banking: Figure 8 depicts the usage of W-SPS in the context of online banking. A client performs online transactions with a bank only after verifying that the bank's server is at a correct location. In this scenario, the banking server acts as the prover and the client-side application is the verifier. The location name service provides the location mapping registered originally by the bank. The banking server contacts the secure positioning infrastructure and obtains a signed location statement. When the client's application connects to the server, it downloads the associated locations from the location name service. Before the client enters its banking credentials, the application initiates a location verification request, during which it verifies the banking server's location. If the verification succeeds, the client proceeds with the transactions.

Drone Navigation and Tracking: The increasing popularity of unmanned aerial vehicles for various applications, e.g., delivery of goods and surveillance, necessitates a secure infrastructure that supports their navigation and tracking. In this scenario, we consider a courier service that uses drones to deliver packages to customers. The courier service needs to continuously track the location of its drones to issue future control commands. The drones use the SPI (Figure 9) to securely determine their position in real-time and forward this information to the courier service. We note that this scenario does not require the use of the location name service which is supported by our modular architecture.

VII. Related Work

In this section, we summarize related work on secure and privacy-preserving location-based services.

Saroiu and Wolman propose the notion of a location proof issued by wireless access points and present its possible applications [78]. Unlike our approach, the wireless infrastructure learns the identity (specifically, the public key) of the device. Lenders et al. discuss the need for location-based trust solutions for mobile applications that leverage secure localization techniques [20]. Canlar et al. proposes CREPUSCOLO, which addresses collusion of entities and privacy preservation in location verification systems using periodically-changing pseudonyms. However, the temporal location of the prover is still revealed to the verifier [79]. The proposals in [80], [81] also suffers the same weakness. Luo and Hengartner propose VeriPlace [82], which requires trusted third parties and preserves location privacy using coarse-grained granularities. In our architecture, the user's location privacy is additionally protected using anonymity sets. Carbunar et al. present similar ideas for privacy-preserving location-based services [83]. However, their positioning system is still not resilient to relay attacks.

VIII. Conclusion

With this paper, we opened a discussion on the need for a novel wide-area secure positioning system to support modern location-based applications. Our proposed W-SPS consists of two main entities: (i) the secure positioning infrastructure, which issues globally verifiable location statements, and (ii) the location name server, which maps user-defined labels to multiple locations. We also introduced protocols that achieve privacy-preserving location verification. Our evaluations also demonstrated the feasibility of such a deployment. As future work, we explore the improvement on the communication range of base stations without compromising the security guarantees and various ways to register and audit location mappings in the location name service.

References

[1] U.S. Department of Defense, "Global positioning system," http://www.gps.gov.

[2] Federal Space Agency of Russia, "Glonass," https://glonass-iac.ru/en/index.php.

[3] European Space Agency, "Galileo," http://www.esa.int/Our_Activities/Navigation/The_future_-_Galileo/What_is_Galileo.

[4] J. E. Elson and D. Estrin, "Time synchronization in wireless sensor networks," Ph.D. dissertation, University of California, Los Angeles, 2003.

[5] J. Elson, L. Girod, and D. Estrin, "Fine-grained network time synchronization using reference broadcasts," *ACM SIGOPS Operating Systems Review*, vol. 36, no. SI, pp. 147–163, 2002.

[6] A. K. Brown and M. A. Sturza, "Vehicle tracking system employing global positioning system (gps) satellites," Jul. 1993, uS Patent 5,225,842.

[7] R. P. Lindsley and C. A. Sharpe, "System for automated toll collection assisted by gps technology," Feb 1996, US Patent 5,490,079.

[8] E. Guizzo, "How google's self-driving car works," *IEEE Spectrum Online, October*, vol. 18, 2011.

[9] "Business Insider: Amazon Is Going To Test Its Delivery Drones In The UK," http://www.businessinsider.com/amazon-is-going-to-test-its-delivery-drones-in-the-uk-2014-11.

[10] E. A. Lee, "Cyber physical systems: Design challenges," in *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on*. IEEE, 2008, pp. 363–369.

[11] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[12] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, 2012.

[13] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[14] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the ION GNSS international technical meeting of the satellite division*, vol. 55, 2008, p. 56.

[15] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Drone hack," *GPS World*, vol. 23, no. 8, pp. 30–33, 2012.

[16] "Ut austin researchers spoof superyacht at sea," http://www.engr.utexas.edu/features/superyacht-gps-spoofing.

[17] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," in *Advances in Cryptology-CRYPTO 2009*. Springer, 2009, pp. 391–407.

[18] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 3. IEEE, 2005, pp. 1917–1928.

[19] H. Koshima and J. Hoshen, "Personal locator services emerge," *Spectrum, IEEE*, vol. 37, no. 2, pp. 41–48, 2000.

[20] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations," in *Proceedings of the 9th workshop on Mobile computing systems and applications*. ACM, 2008, pp. 60–64.

[21] U.S. Department of Defense, "Information about gps jamming," http://www.gps.gov/spectrum/jamming/.

[22] W. T. Dickinson, "The LORAN-C system of navigation," 1962.

[23] "Google maps," https://maps.google.com.

[24] "Bing maps," https://www.bing.com/maps.

[25] D. J. Torrieri, *Statistical theory of passive location systems*. Springer, 1990.

[26] "Omega (navigation system)," http://www.jproc.ca/hyperbolic/omega.html.

[27] J. Shokouh, "Detecting gnss attacks on smartphones," 2013.

[28] N. O. Tippenhauer, K. B. Rasmussen, C. Pöpper, and S. Čapkun, "Attacks on public wlan-based positioning systems," in *Proceedings of the 7th international conference on Mobile systems, applications, and services*. ACM, 2009, pp. 29–40.

[29] M. Psiaki, S. Powell, and B. O'Hanlon, "Correlating Carrier Phase with Rapid Antenna Motion," 2013.

[30] D. M. Akos, "Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)," *Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[31] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[32] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, 2003.

[33] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," in *Proceedings of the ION International Technical Meeting*, 2009.

[34] M. Schäfer, V. Lenders, and J. Schmitt, "Poster: Secure path verification using mobility-differentiated toa."

[35] R. Poovendran, C. Wang, and S. Roy, *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*. Springer, 2006.

[36] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks," in *Workshop on Security of Ad Hoc and Sensor Networks (SASN)*. ACM, Oct. 2003, pp. 21–32.

[37] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *WISE03*. New York, NY, USA: ACM, September 2003, pp. 1–10.

[38] G. P. Hancke, "Design of a secure distance-bounding channel for RFID," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 877–887, May 2011.

[39] "3db access AG," http://www.3db-technologies.com/.

[40] N. O. Tippenhauer, "Physical-Layer Security Aspects of Wireless Localization," Ph.D. dissertation, ETH Zurich, Switzerland, 2012.

[41] International Organization for Standardization, "ISO 3166: Codes for countries and their subdivisions," International Standard.

[42] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, ser. EUROCRYPT '93. Springer-Verlag New York, Inc., May 1993, pp. 344–359.

[43] N. O. Tippenhauer and S. Čapkun, "ID-based Secure Distance Bounding and Localization," in *Proceedings of the 14th European Conference on Research in Computer Security*. Berlin, Heidelberg: Springer-Verlag, Sep. 2009, pp. 621–636.

[44] Y.-J. Tu and S. Piramuthu, "RFID Distance Bounding Protocols," in *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, Sep. 2007.

[45] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Sep. 2005, pp. 67–73.

[46] K. B. Rasmussen and S. Čapkun, "Realization of RF Distance Bounding," in *Proceedings of the 19th USENIX Security Symposium*, Aug. 2010, pp. 389–402.

[47] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels," *ACM Journal on Wireless Communications and Mobile Computing*, vol. 8, no. 9, pp. 1227–1232, Nov. 2008.

[48] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, Mar. 2007, pp. 204–213.

[49] L. Bussard and W. Bagga, "Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks," in *Proceedings of 20th International Conference on Security and Privacy in the Age of Ubiquitous Computing*, May 2005, pp. 223–238.

[50] D. Singelée and B. Preneel, "Distance bounding in noisy environments," in *Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks*. Berlin, Heidelberg: Springer-Verlag, Jul. 2007, pp. 101–115.

[51] J. Clulow, G. Hancke, M. Kuhn, and T. Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," in *Proceedings of the 3rd European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks*, ser. Lecture Notes in Computer Science. Springer, Sep. 2006, pp. 83–97.

[52] G. P. Hancke and M. G. Kuhn, "Attacks on time-of-flight Distance Bounding Channels," in *Proceedings of the 1st ACM Conference on Wireless Network Security*. ACM, Apr. 2008, pp. 194–202.

[53] S. Sedighpour, S. Capkun, S. Ganeriwal, and M. B. Srivastava, "Distance enlargement and reduction attacks on ultrasound ranging," in *Proceedings of the 3rd ACM Conference on Embedded Networked Sensor Systems*. New York, NY, USA: ACM, Nov. 2005.

[54] *IEEE 802.15.4a-2007 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, The Institute of Electrical and Electronic Engineers, 2007.

[55] *ISO/IEC 24730-5 Information technology – Real-time locating systems (RTLS) – Part 5: Chirp spread spectrum (CSS) at 2.4 GHz air interface*, The Institute of Electrical and Electronic Engineers, 2010.

[56] A. J. Berni and W. D. Gregg, "On the Utility of Chirp Modulation for Digital Signaling," *IEEE Transactions on Communications*, vol. 21, no. 6, pp. 748–751, Jun. 1973.

[57] C. E. Cook and M. Bernfeld, *Radar signals: An introduction to theory and application*. Academic Press, New York, 1967.

[58] J. Peck, "SONAR–The RADAR of the Deep," in *Popular Science*, Nov. 1945, vol. 147, no. 5.

[59] A. Springer, W. Gugler, M. Huemer, L. Reindl, C. C. W. Ruppel, and R. Weigel, "Spread Spectrum Communications Using Chirp Signals," in *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*, May 2000, pp. 166–170.

[60] *NanoLOC TRX Transceiver (NA5TR1) Datasheet Version 2.3*, Nanotron Technologies GmbH, 2010.

[61] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-layer attacks on chirp-based ranging systems," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2012, pp. 15–26.

[62] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec, "Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures," *IEEE Transactions on Wireless Communications*, vol. 10, no. 4, pp. 1334–1344, Apr. 2011.

[63] ——, "The Cicada Attack: Degradation and Denial of Service in IR Ranging," in *Proceedings of 2010 IEEE International Conference on Ultra-Wideband*, vol. 2, Sep. 2010, pp. 1–4.

[64] *Sapphire Dart Ultra-Wideband (UWB) Real Time Locating System*, http://www.zebra.com, Zebra Technologies, 2010.

[65] *Ubisense Real-time Location Systems (RTLS)*, http://www.ubisense.net/en/rtls-solutions, Ubisense Technologies, 2010.

[66] "DecaWave: Precise Indoor Location and RTLS," http://www.decawave.com/.

[67] "Time Domain: Ultra wideband ranging, communications and radar," http://www.timedomain.com/.

[68] S. Capkun, M. Srivastava, and M. Cagalj, "Securing localization with hidden and mobile base stations," in *IEEE Conference on Computer Communications (INFOCOM)*, 2006.

[69] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "Information security and cryptology — icisc 2008." Berlin, Heidelberg: Springer-Verlag, 2009, ch. The Swiss-Knife RFID Distance Bounding Protocol, pp. 98–115.

[70] S. Vaudenay, "On modeling terrorist frauds," in *Provable Security*. Springer, 2013, pp. 1–20.

[71] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology EUROCRYPT 2001*, ser. Lecture Notes in Computer Science, B. Pfitzmann, Ed. Springer Berlin Heidelberg, 2001, vol. 2045, pp. 93–118.

[72] ——, "A signature scheme with efficient protocols," in *Security in Communication Networks*, ser. Lecture Notes in Computer Science, S. Cimato, G. Persiano, and C. Galdi, Eds. Springer Berlin Heidelberg, 2003, vol. 2576, pp. 268–289.

[73] J. Camenisch, R. Chaabouni, and a. shelat, "Efficient protocols for set membership and range proofs," in *Advances in Cryptology - ASIACRYPT 2008*, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed. Springer Berlin Heidelberg, 2008, vol. 5350, pp. 234–252.

[74] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 21–30.

[75] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in CryptologyCRYPTO86*. Springer, 1987, pp. 186–194.

[76] P. Bichsel, J. Camenisch, T. Groß, and V. Shoup, "Anonymous credentials on a standard java card," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 600–610.

[77] "JVM monitor," JVMMonitor.

[78] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*. ACM, 2009, p. 3.

[79] E. S. Canlar, M. Conti, B. Crispo, and R. Di Pietro, "Crepuscolo: A collusion resistant privacy preserving location verification system," in *Risks and Security of Internet and Systems (CRiSIS), 2013 International Conference on*. IEEE, 2013, pp. 1–9.

[80] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1889–1897.

[81] M. Talasila, R. Curtmola, and C. Borcea, "Link: Location verification through immediate neighbors knowledge," in *Mobile and Ubiquitous Systems: Computing, Networking, and Services*. Springer, 2012, pp. 210–223.

[82] W. Luo and U. Hengartner, "Veriplace: a privacy-aware location proof architecture," in *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM, 2010, pp. 23–32.

[83] B. Carbunar, R. Sion, R. Potharaju, and M. Ehsan, "The shy mayor: Private badges in geosocial networks," in *Applied Cryptography and Network Security*. Springer, 2012, pp. 436–454.