Secure Location Verification: Why You Want Your Verifiers to be Mobile

Matthias Schäfer[1], Carolina Nogueira[1], Jens B. Schmitt[1], and Vincent Lenders[2]

[1] DISCO Labs, TU Kaiserslautern, Germany
{schaefer, nogueira, jschmitt}@uni-kl.de
[2] armasuisse, Switzerland
vincent.lenders@armasuisse.ch

Abstract. The integrity of location information is crucial in many applications such as access control or environmental sensing. Although there are several solutions to the problem of secure location verification, they all come with expensive requirements such as tight time synchronization, cooperative verification protocols, or dedicated hardware. Yet, meeting these requirements in practice is often not feasible which renders the existing solutions unusable in many scenarios. We therefore propose a new solution which exploits the *mobility of verifiers* to verify locations. We show that mobility can help minimize system requirements while at the same time achieves strong security. Specifically, we show that two moving verifiers are sufficient to securely verify location claims of a static prover without the need for time synchronization, active protocols, or otherwise specialized hardware. We provide formal proof that our method is secure with minimal effort if the verifiers are able to adjust their movement to the claimed location ("controlled mobility"). For scenarios in which controlled mobility is not feasible, we evaluate how more general claim-independent movement patterns of verifiers affect the security of our system. Based on extensive simulations, we propose simple movement strategies which improve the attack detection rate up to 290% with only little additional effort compared to random (uncontrolled) movements.

1 Introduction

Many real-world distributed systems require sharing of location information among network nodes. For example, in location-based access control or environmental sensing applications, the location of individual nodes is often crucial for distributed coordination, service delivery or decision making.

A common approach to sharing location information with neighboring nodes is broadcasting them periodically over a wireless link (e.g., ADS-B, AIS, RTK, WiFi, or Bluetooth). While this method has advantages in terms of simplicity and scalablity, a known weakness of this scheme is that nodes may (intentionally or not) advertise wrong location claims. In order to detect such false location information, secure location verification schemes have been proposed in the literature with the aim to securely verify whether the advertised ("claimed") location corresponds to the real position of the sender. Since Brands and Chaum first addressed this problem in 1993 [2] and Sastry et al. later defined location (or in-region) verification in 2003 [12], many solutions and methods have been proposed in the literature to solve this problem. The existing solutions can broadly be classified into methods based on distance bounding [2, 12, 19, 15, 20, 10], time-difference of arrival measurements (TDoA) [19, 22, 16, 1], angle of arrival measurements [6, 8], or hybrid methods [4, 3].

All of these techniques have in common that they verify location claims by checking physical properties of the transmitted radio signals. For example, distance bounding protocols or TDoA systems exploit the fact that a radio signals cannot propagate faster than the speed of light. A location claim violating this condition must be false. While the majority of these schemes have been shown to be secure within their assumptions, the requirements to the underlying systems limit their applicability significantly. More specifically, TDoA-based methods generally require many verifiers and tight time synchronization between verifiers. This is usually achieved by additional infrastructure (e.g. wired networks) and the exchange of synchronization information between nodes. This dependency, however, significantly reduces the flexibility and increases the communication overhead, rendering the approaches unsuitable for ad hoc or mobile scenarios, especially when energy supply is limited. Distance bounding and angle of arrival measurements, on the contrary, do not require time synchronization. However, since they rely on active verification protocols and specialized hardware (see [11] for more details), we argue that their applicability is also limited. For example, they cannot be applied to systems that are already in place such as mobile phones. Upgrading the billions of smartphones in use today to meet the requirements of distance bounding seems rather impracticable.

In our prior works [13] and [14], we have shown that by adding mobility of nodes to the model, requirements of similar verification systems can be lowered significantly. More specifically, we have shown that tracks and motion of *moving provers* can be verified without any of the aforementioned limitations while at the same time strong security can be provided. However, the downside of these approaches is that they are only applicable to scenarios with *moving provers*. They are not applicable to the classic location verification problem which considers *stationary provers* at single locations or within certain areas.

In this work, we bridge this gap by bringing the benefits of mobility to the problem of verifying single locations. We present a novel method based on *mobile verifiers* which achieves strong security without limiting the attacker's knowledge (i.e., no "security by obscurity") nor does it rely on time synchronization or active verification protocols. We introduce the concept of "controlled mobility" and show that by being able to adjust the verifiers' movements to the claimed locations, provable security can be achieved with just two verifiers and two location claim transmissions. Compared to existing approaches, this is both lightweight and fast. In addition to that, we also analyze more general movement strategies for scenarios that require batch verification, i.e., the simultaneous verification of multiple location claims. We conducted extensive simulations to find claim-independent movement strategies which maximize security while at the same time minimize resources and overhead. Our results indicate that by using specific movement patterns, only three verifiers or four location claim transmissions are required to achieve a 100% detection rate.

The remainder of this paper is organized as follows. In section 2, we provide a detailed problem and system description as well as a real-world example which matches this model. Section 3 then introduces our location verification protocol based on the mobility-differentiated time of arrival as well as the concept of controlled mobility. The security of this concept is then formally analyzed in section 4. Afterwards, in section 6, we extend our analysis by evaluating the security of our scheme in uncoordinated scenarios. Finally, we discuss and compare related methods in section 7.

2 System Model & Notation

2.1 Problem Statement

In line with the definition by Sastry et al. [12], we define the problem of secure location verification as follows. A set of verifiers $\mathcal{V} = \{\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_n\}$ wishes to check whether a prover $\mathcal{P}$ is at a location l of interest.

2.2 System Model

We assume that verifiers are moving while $\mathcal{P}$ advertises its location $m > 1$ times. This implies that each transmission is received by the verifiers from different locations. To minimize the verification overhead, we also assume that verifiers are passive receivers and there is no communication between prover and verifiers other than the prover's location advertisements. We further assume that the inter-transmission time $\Delta^{i,i+1}$ of two subsequent location advertisements is known to each verifier. This can be achieved by either using a predefined constant interval Δ, i.e., $\Delta^{(i,i+1)} = \Delta$ for all i, or by having the prover include transmission timestamps $t_{\mathcal{P}}^{(i)}$ in the location claim broadcasts, i.e., $\Delta^{i,i+1} = t_{\mathcal{P}}^{(i+1)} - t_{\mathcal{P}}^{(i)}$. It is worth noting that the first option reduces the communication overhead since less information needs to be transmitted by the prover while the second option provides much more flexibility, e.g., to support random medium access protocols such as ALOHA. Finally, we assume that each verifier knows its location at all times and has a stable but *unsynchronized* local clock.

2.3 Threat Model

We consider all information coming from the prover as untrustworthy. More specifically, we consider a malicious prover (adversary) which has full control over the reported timestamps $t_{\mathcal{P}}^{(i)}$, the real transmission intervals $\Delta_{\mathcal{A}}^{(i,j)}$, and the actual claimed location l. As l is the actual property of interest here, we assume that the adversary is located at a location different from the claimed location, i.e., $\mathcal{A} \neq l$.[3]

[3] As for verifiers and prover, we use $\mathcal{A}$ interchangeably for the adversary's identity and location whenever the meaning is clear from the context.

As we aim at strong security rather than security by obscurity, we do not limit the adversary's knowledge. In effect, our adversary has perfect knowledge of the verifiers' locations at any point in time and it can even predict the verifiers' future locations. This assumption is an important difference from the ranging-based scheme proposed by Čapkun et al. in [21], where security is based on the adversary's lack of knowledge of the "hidden" verifiers' location.

Finally, we assume that the verifiers are not compromised and they have secure means to determine their locations. Consequently, we can consider locations $\mathcal{V}_a^{(i)}$ and timestamps $t_a^{(i)}$ of the verifiers trustworthy for all $a \in \{1, \ldots, n\}$ and $i \in \{1, \ldots, m\}$.

2.4 Use Cases

A specific real-world example for a system that could (and should) be extended with our verification scheme are navigational aid systems used in aviation such as non-directional radio beacons (NDB) or VHF omnidirectional radio range (VOR) [7]. In both systems, ground stations at fixed locations transmit signals that are used by aircraft for navigation. Each transmitter is assigned a unique identifier that can be used by pilots and onboard systems to look up the station's location. Once their location is known, aircraft use them to stay on track by flying towards or in a certain angle to the ground station.

As is the case with most systems used in aviation, security has not been part of the design of NDB and VOR. As a consequence, they are highly vulnerable to spoofing attacks which can be used to mislead pilots or automatic flight control systems [17]. Although many aircraft have more accurate means of navigation (GPS), many pilots around the world still rely on these systems. Our verification scheme could be used to mitigate this threat in a scalable and light-weight manner. The ground transmitters can be considered as stationary provers while aircraft equipped with additional means of positioning (GPS) can act as moving verifiers. Onboard verification systems can then detect fake signals and inform ground personnel and other pilots.

Another use case is access control for services which should only be available to users within a certain physically restricted area. For instance, addtional premium information about a sports match could be offered in a mobile app to fans within a stadium. To prevent that people on the outside have access to that service, drones or moving cameras can be used to verify that people are in the stadium. Moreover, existing wireless technologies such as Bluetooth or WiFi could be used by the app for verification without the need for additional hardware.

3 Location Verification Protocol (MoVers)

In order to claim a location, a prover $\mathcal{P}$ broadcasts its location $m > 1$ times with pre-defined inter-transmission times $\Delta^{(i-1,i)}$ $(i = 2 \ldots m)$. For the sake of simplicity, we use a constant inter-transmission time Δ, i.e., $\Delta^{(i-1,i)} = \Delta$ for all $i = 2 \ldots m$ (see Section 2). On reception of $\mathcal{P}$'s i-th transmission $(1 < i \leq m)$, each verifier $\mathcal{V}_a$ stores its current location $\mathcal{V}_a^{(i)}$ and receiver timestamp $t_a^{(i)}$.

The verification protocol is based on the following condition: for all $i > 1$, all verifiers check whether the verification condition

$$\varDelta_a^{(i-1,i)} \overset{?}{=} \varDelta + (\delta_a^{(i)} - \delta_a^{(i-1)}) \tag{1}$$

holds. They estimate the propagation delay $\delta_a^{(i)}$ using the known positions, i.e., $\delta_a^{(i)} = dist(\mathcal{V}_a^{(i)}, \mathcal{P})/c$ with $dist(\cdot,\cdot)$ denoting the Euclidean distance between two locations and c the signal propagation speed (usually speed of light). If the equation is satisfied, the verifier remains silent. Otherwise it raises an alarm. The verification procedure terminates successfully, i.e., $\mathcal{P}$'s location is verified, after m transmissions without any alarm.

3.1 Controlled Mobility

We assume that the verifiers are changing their locations between the location claim transmissions, i.e., $\mathcal{V}_a^{(i)} \neq \mathcal{V}_a^{(i-1)}$. Verifiers can choose their next location $\mathcal{V}_a^{(i)}$ within the physical limitations using different strategies. We call this conscious choice of the next position "controlled mobility" (as opposed to "opportunistic" or "random" mobility) and distinguish between *coordinated* and *uncoordinated* controlled mobility. In coordinated controlled mobility, verifiers choose their direction of movement collaboratively to maximize security. To avoid communication overhead, we assume that verifiers coordinate their movements solely based on the claimed location and some fixed identifier. In the following security analysis, we derive such a coordinated movement pattern and prove its security. The disadvantage of this approach, however, is that the verification of multiple location claims simultaneously ("batch verification") is not possible. While this is not a requirement per se, there are scenarios with many participants (e.g., verifying people's locations in a stadium) that require a more scalable approach. We therefore extend our analysis with simulations evaluating more general uncoordinated (yet controlled) movement patterns that allow for batch verification. Based on our results, we can provide heuristics for verifier movements that maximize security while preserving a high efficiency in terms of verification time and minimum required number of verifiers.

4 Security Analysis

The two main design goals of our protocol are *security* and *efficiency*. While security as a goal is inherent to the problem, efficiency in terms of resources and verification time is crucial for the protocol's applicability in mobile scenarios. For instance, using antenna arrays for beamforming or high performance computers for complex algorithms on mobile nodes such as drones is impracticable since both weight and energy consumption must be low to maintain adequate operating times. We therefore start our security analysis by setting up the theoretical foundations and then successively increase the transmission time (in terms of number of transmissions) and number of verifiers until security is established. In this way, we obtain the fastest and most resource-efficient configuration that can provide strong security. For the sake of presentation, we conduct our analysis in two-dimensional space. Extending the results to three dimensions is straightforward.

4.1 Single Verifier

In order to let an adversary's location claims appear genuine to a verifier $\mathcal{V}_a$, Eq. (1) must be met for all $i = 2, \ldots, m$. In particular, if the adversary wants to spoof a certain location $\mathcal{P}$ from its location $\mathcal{A}$, it needs to choose its inter-transmission intervals such that

$$\varDelta_{\mathcal{A}}^{(i-1,i)} + (\delta_{\mathcal{A},a}^{(i)} - \delta_{\mathcal{A},a}^{(i-1)}) = \varDelta + (\delta_a^{(i)} - \delta_a^{(i-1)})$$

holds, where $\delta_{\mathcal{A},a}^{(i)} = \mathit{dist}(\mathcal{A}, \mathcal{V}_a)/c$ is the propagation delay of the i-th transmission from the adversary to verifier $\mathcal{V}_a$. Considering only a single verifier, this can easily be achieved by simply choosing

$$\begin{aligned} \varDelta_{\mathcal{A}}^{(i-1,i)} &= \varDelta + (\delta_a^{(i)} - \delta_a^{(i-1)}) - (\delta_{\mathcal{A},a}^{(i)} - \delta_{\mathcal{A},a}^{(i-1)}) \\ &= \varDelta_a^{(i-1,i)} - (\delta_{\mathcal{A},a}^{(i)} - \delta_{\mathcal{A},a}^{(i-1)}) \ . \end{aligned} \tag{2}$$

In other words, the adversary can simply compensate for its unexpected propagation delays to $\mathcal{V}_a$ by choosing an inter-transmission interval equal to the difference of the expected from the actual inter-arrival time. *We conclude that a single verifier cannot provide any security since an adversary can spoof arbitrary locations.*

We point out that this result is equal to the case of a single verifier in [13]. The only difference is that in [13], a moving sender is considered whereas here we assume that the receiver moves. However, by adding another verifier in the next step of our analysis, we diverge from the analysis in [13] since we then face multiple moving nodes in our system whereas [13] always considers just a single moving node. Facing multiple mobile nodes increases the complexity of the analysis significantly.

4.2 Two Verifiers

We now consider a system with two verifiers $\mathcal{V}_a$ and $\mathcal{V}_b$. Then, Eq. (2) must be satisfied by $\varDelta_{\mathcal{A}}^{(i-1,i)}$ for both verifiers, i.e.,

$$\begin{aligned} \varDelta_{\mathcal{A}}^{(i-1,i)} &= \varDelta_a^{(i-1,i)} + (\delta_{\mathcal{A},a}^{(i)} - \delta_{\mathcal{A},a}^{(i-1)}) \\ \varDelta_{\mathcal{A}}^{(i-1,i)} &= \varDelta_b^{(i-1,i)} + (\delta_{\mathcal{A},b}^{(i)} - \delta_{\mathcal{A},b}^{(i-1)}) \end{aligned}$$

must both hold for all $i = 2, \ldots, m$. By equating both constraints, re-arranging and plugging Eq. (1) into them, we can conclude that such a $\varDelta_{\mathcal{A}}^{(i-1,i)}$ exists if and only if the following requirement is met:

$$\begin{aligned} &(\delta_{\mathcal{A},a}^{(i)} - \delta_{\mathcal{A},a}^{(i-1)}) - (\delta_{\mathcal{A},b}^{(i)} - \delta_{\mathcal{A},b}^{(i-1)}) \\ &\qquad = \varDelta_a^{(i-1,i)} - \varDelta_b^{(i-1,i)} \\ &\qquad = (\delta_a^{(i)} - \delta_a^{(i-1)}) - (\delta_b^{(i)} - \delta_b^{(i-1)}) \end{aligned} \tag{3}$$

This means that the inter-transmission interval $\varDelta_{\mathcal{A}}^{(i-1,i)}$ only exists if the adversary is either located at a position where the differences of distances[4] to each verifier changes between two consecutive transmissions exactly by the same amount as the differences of distances from $\mathcal{P}$ to $\mathcal{V}_a$ and $\mathcal{V}_b$. Alternatively, since the adversary is clairvoyant, it can also try to find and claim a location $\mathcal{P}$ (e.g.,

[4] We interpret propagation delays as direct representatives of distances.

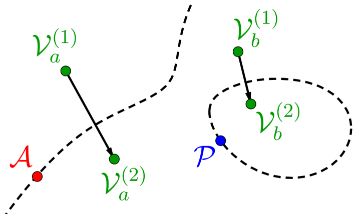


Fig. 1. Example scenario with two verifiers and the resulting restrictions (implicit curve) for the adversary's location $\mathcal{A}$.

within an area of interest) which satisfies this constraint. From a mathematical point of view both strategies are equal since the adversary either tries to find an $\mathcal{A}$ (left-hand side of Eq. (3)) which matches a given $\mathcal{P}$ (right-hand side) or vice versa.

From the verifier perspective, however, it makes more sense to analyze whether for a given $\mathcal{P}$ there is a location $\mathcal{A} \neq \mathcal{P}$ which also satisfies Eq. (1) for all verifiers. Hence, without loss of generality, we further analyze the existence of such a location $\mathcal{A}$ given a claimed location $\mathcal{P}$. Since $\mathcal{P}$ and the verifier's locations can be considered fix in that case, the only free parameter left in Eq. (3) is $\mathcal{A}$ and we therefore summarize its right-hand side by a constant

$$k_{\mathcal{P}}^{(i)} = (\delta_a^{(i)} - \delta_a^{(i-1)}) - (\delta_b^{(i)} - \delta_b^{(i-1)})$$

which yields the requirement

$$(\delta_{\mathcal{A},a}^{(i)} - \delta_{\mathcal{A},a}^{(i-1)}) = (\delta_{\mathcal{A},b}^{(i)} - \delta_{\mathcal{A},b}^{(i-1)}) + k_{\mathcal{P}}^{(i)} \qquad (4)$$

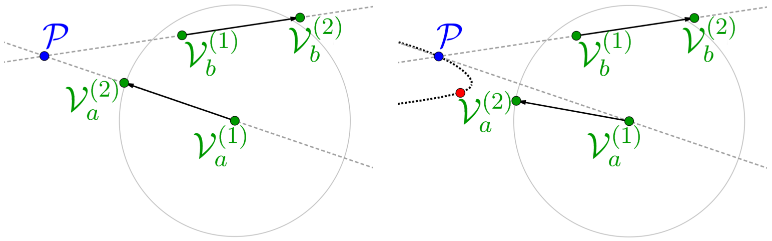
for two consecutive transmissions of a false claim. As a result, $\mathcal{P}$ can be spoofed from all locations $\mathcal{A}$ at which the distance change between two transmissions from $\mathcal{A}$ to $\mathcal{V}_a$ differs exactly by $k_{\mathcal{P}}^{(i)}$ from that to $\mathcal{V}_b$.

Fig. 1 shows an example scenario with two transmissions of location claims for $\mathcal{P}$, two verifiers, and the implicit curve defined by Eq. (4) (dashed line). A possible location $\mathcal{A}$ of an adversary is also indicated by a red dot, although it could be anywhere on the dashed line. It is worth mentioning that $\mathcal{P}$ is by construction on the implicit curve. While this is natural since the legitimate $\mathcal{P}$ must satisfy the above constraint, the curve's continuity implies that there are locations within a potential area of interest (e.g., nearby $\mathcal{P}$) where an adversary could be located without being detected.

We conclude that for two verifiers, the adversary's degree of freedom is reduced to the implicit curve described by Eq. (4). In particular, MoVers is only secure for two verifiers, if this equation is satisfied by no location other than $\mathcal{P}$.

4.3 More verifiers or more transmissions

Analogously to the previous step, each additional verifier ($|\mathcal{V}| \geq 3$) or location claim ($m \geq 3$) further restricts the adversary since they add more equations such as Eq. (4) to the system. Similarly to the previous case, the adversary has to be positioned on several curves at the same time. In fact, the adversary is then limited to a (finite) set of unconnected points rather than a curve. In order to spoof a location, a clever adversary would compute the implicit curves before-



(a) Movement pattern according to Theorem 1. The implicit curve defined by Eq. (4) is reduced to $\mathcal{P}$.

(b) Deviations from the movement pattern according to Theorem 1 may result in vulerabilities to spoofing attacks.

Fig. 2. Security Through Coordinated Controlled Mobility

hand and then try to find such an intersection different from $\mathcal{P}$. However, the probability that these erratic implicit curves intersect more than once becomes increasingly unlikely with each additional verifier or transmission.

Since an analytical exploration of the behavior of these intersections is extremely challenging (if not impossible), we now focus our analysis on coordinated controlled mobility and then revisit the behavior and existence of such intersections in our simulations in Section 6.

5 Coordinated Controlled Mobility

In scenarios where verifiers are able to adapt their movements to a claimed location, they have some degree of control over the implicit curves and thus the adversary's constraints. In the optimal case, the verifiers change their locations in a way such that the resulting implicit curves (Eq. (4)) only intersect at $\mathcal{P}$. If this is achieved, MoVers is secure since an adversary located at $\mathcal{A} \neq \mathcal{P}$ would violate the verification check Eq. (1) for at least one verifier according to our above analysis. In the following, we propose such a movement pattern and prove its security.

Theorem 1. *If one verifier moves exactly towards $\mathcal{P}$ while another one moves exactly away from $\mathcal{P}$ and not in line with the first one, then* MoVers *is secure for $m = 2$.*

Proof. Let two verifiers $\mathcal{V}_a, \mathcal{V}_b \in \mathcal{V}$ and two transmissions by a prover claiming location $\mathcal{P}$ be given. Without loss of generality, we assume that $\mathcal{V}_a$ is the verifier heading directly towards and $\mathcal{V}_b$ directly away from $\mathcal{P}$. More formally, let $\boldsymbol{v}_{a/b} = (\mathcal{V}_{a/b}^{(2)} - \mathcal{V}_{a/b}^{(1)})$ be the vectors describing the position changes of the two verifiers between the two transmissions. Then there is an $s_a \in \mathbb{R}$ with $s_a > 0$ such that

$$\mathcal{P} = \mathcal{V}_a^{(1)} + \boldsymbol{v}_a \cdot s_a \ .$$

Similarly, there is an $s_b \in \mathbb{R}$ with $s_b < 0$ such that

$$\mathcal{P} = \mathcal{V}_b^{(1)} + \boldsymbol{v}_b \cdot s_b \ .$$

We further assume that the two verifiers are not in line with each other, i.e., there is no $s \in \mathbb{R}$ such that

$$\mathcal{V}_b^{(1)} = \mathcal{V}_a^{(1)} + \boldsymbol{v}_a \cdot s \ .$$

An example scenario showing such a movement is depicted in Fig. 2a. Under these circumstances, the absolute distance change between $\mathcal{P}$ and $\mathcal{V}$ is maximal and thus the estimated propagation delays from the prover to both verifiers change by the maximum possible absolute values

$$\delta_a^{(2)} = \delta_a^{(1)} - \frac{\|\boldsymbol{v}_a\|}{c} \qquad \text{and} \qquad \delta_b^{(2)} = \delta_b^{(1)} + \frac{\|\boldsymbol{v}_b\|}{c} \ ,$$

since both distances change exactly by the full movements' lengths by the verifiers between the transmissions, yet, in opposite directions. Additionally, $\frac{\|\boldsymbol{v}_a\|}{c} \leq \delta_a^{(2)} - \delta_a^{(1)}$ is required, meaning that $\mathcal{V}_a$ should not move beyond $\mathcal{P}$. Plugging this into Eq. 1 yields

$$\begin{aligned} \Delta_a^{(1,2)} &\overset{?}{=} \Delta + (\delta_a^{(2)} - \delta_a^{(1)}) \\ &= \Delta - \frac{\|\boldsymbol{v}_a\|}{c} \end{aligned}$$

and, analogously, $\Delta_b^{(1,2)} \overset{?}{=} \Delta + \frac{\|\boldsymbol{v}_b\|}{c}$.

Let us now consider an adversary located at $\mathcal{A} \neq \mathcal{P}$. In order to pass the verification checks of the two verifiers, it has to choose $\Delta_{\mathcal{A}}^{(1,2)}$ such that the two equations

$$\Delta_{\mathcal{A}}^{(1,2)} + (\delta_{\mathcal{A},a}^{(2)} - \delta_{\mathcal{A},a}^{(1)}) = \Delta - \frac{\|\boldsymbol{v}_a\|}{c} \tag{5}$$

$$\underbrace{\Delta_{\mathcal{A}}^{(1,2)} + (\delta_{\mathcal{A},b}^{(2)} - \delta_{\mathcal{A},b}^{(1)})}_{\text{“real” signal propagation}} = \Delta + \frac{\|\boldsymbol{v}_b\|}{c} \tag{6}$$

are satisfied. Let us now assume $\mathcal{A}$ would not be located in line with $\mathcal{V}_a$ and $\mathcal{P}$. Then

$$\delta_{\mathcal{A},a}^{(2)} - \delta_{\mathcal{A},a}^{(1)} > -\frac{\|\boldsymbol{v}_a\|}{c}$$

holds, since $\mathcal{V}_a$ does not move exactly towards $\mathcal{A}$. This means for the adversary that it has to choose $\Delta_{\mathcal{A}}^{(1,2)} < \Delta$ to compensate for the difference. Yet, then it cannot satisfy Eq. 6 since it would be required that

$$\delta_{\mathcal{A},b}^{(2)} - \delta_{\mathcal{A},b}^{(1)} > \frac{\|\boldsymbol{v}_b\|}{c}.$$

However, given the distance moved by $\mathcal{V}_b$ between the two transmissions and the associated maximum possible distance change of $\|\boldsymbol{v}_b\|$, this is impossible. Hence, $\mathcal{A}$ must be located in line with $\mathcal{V}_a$.

We can show analogously that $\mathcal{A}$ must also be in line with $\mathcal{P}$ and $\mathcal{V}_b$ in order to satisfy Eq. 5. As a consequence, $\mathcal{A}$ must be located on two lines which both cross $\mathcal{P}$. Since $\mathcal{V}_a$ and $\mathcal{V}_b$ are not in line with each other, these two lines are different. Since furthermore two different lines can only have one intersection, we can conclude that $\mathcal{P}$ is the only location from which a sender can satisfy both equations at the same time. Thus, Theorem 1 holds and MoVers is secure.

We conclude that by adapting the verifiers' movements to the claimed location ("coordinated controlled mobility"), *MoVers can provide provable security with an efficient configuration of two verifiers and two transmissions.*

Summary: The key results from this theoretical analysis are that (i) a single verifier cannot provide any security, (ii) two verifiers can provide provable security with coordinated controlled mobility (Theorem 1), and (iii) the security increases with each additional transmission or verifier as more restrictions are added for the adversary's location.

6 Uncoordinated Mobility

As explained in Section 3.1, coordinated controlled mobility can only be used if there is only one location to be verified at a time. For scenarios with more than one prover, a movement strategy independent from $\mathcal{P}$ is required. So far we considered only two transmissions of the location claim in the presence of two verifiers. As we know from Section 4, having more than two verifiers ($n > 2$) or more than two transmissions ($m > 2$), each reduces the degree of freedom for the adversary by adding more implicit curves to the constraints for $\mathcal{A}$. More specifically, since the verifiers move between each transmission, the focal points for the implicit curve defined by Eq. (4) change for every $i \in \{2, \ldots, m\}$ and each pair $\mathcal{V}_a, \mathcal{V}_b \in \mathcal{V}$. As a result, $\mathcal{A}$ needs to be located at an intersection of $(m-1) \cdot \binom{n}{2}$ different implicit curves in order to remain undetected when claiming $\mathcal{P} \neq \mathcal{A}$. Moreover, this set of intersections can be assumed to be finite since the curves are not periodic. The number of such intersections can be considered a direct measure of the attacker's degree of freedom and thus the security of our scheme. Our scheme is in particular secure if there is only one intersection of all curves (which is $\mathcal{P}$ by construction) since false claims will then violate Eq. (1) for at least one verifier.

Most related problems are of a simple hyperbolic nature (e.g. [13, 14, 18]) and can often be analyzed algebraically. Unfortunately, having more than one mobile node makes the exact analysis hard because each moving element contributes to the equations. For example, in contrast to the analysis of intersections of a set of hyperbolas, which is common, e.g., for TDoA or ranging-based approaches, we face curves defined by intersections of intersections of hyperbolas with multiple parameters. These curves are of a higher order than hyperbolas which makes an exact analysis of the intersections extremely difficult. Although there exist methods to decrease the computational complexity when computing the intersection of hyperbolas (e.g., homogeneous coordinates [9]), we could not find any analytical method to analyze it in a general way, since the parameters that may determine the hyperbolas are unknown. We therefore continue our analysis by extending our theoretical findings with simulations analyzing the behavior of the intersections with respect to the verifiers' movements independent from $\mathcal{P}$.

In the following simulations, we differentiate between opportunistic and (uncoordinated) controlled mobility. In opportunistic (or random) mobility, nodes are not moving according to any predefined pattern. This reflects scenarios where uncontrolled nodes act as verifiers (e.g., cellphones, agricultural machines, or

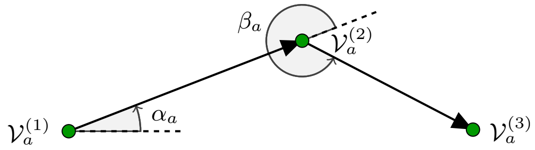


Fig. 3. Description of a verifier $\mathcal{V}_a$'s movement in our simulations. The initial direction is the counter-clockwise angle α_a relative to a horizontal axis through $\mathcal{V}_a^{(1)}$. After the initial step (i.e., for $i > 1$), we only consider the direction changes (β_a, γ_a, ...), i.e., the counter-clockwise angle between the old and the new direction.

airplanes). In controlled mobility, verifiers follow certain patterns aiming at improving the security of the verification scheme.

6.1 Simulation Design

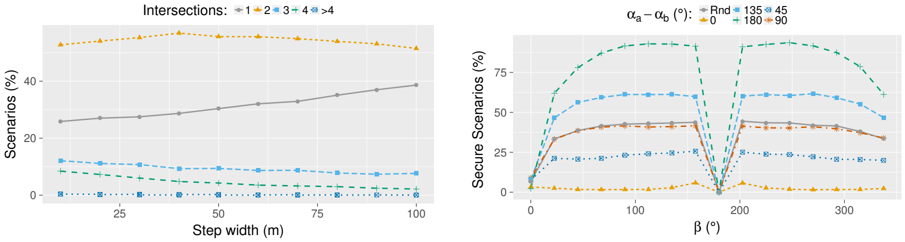
We implemented a simulation framework in MATLAB® which allows us to analyze the intersections for arbitrary constellations of verifiers and provers. By controlling the movement of verifiers between the reception of location claims, we show the effect of the geometry on the security of our approach and identify beneficial movement strategies for verifiers.

In accordance with our verification process, we implemented our simulations as a discrete-event simulation. The events are the transmissions of a location claim and we recorded the locations of all n verifiers at each transmission. Based on the recorded locations and $\mathcal{P}$ we then setup the nonlinear equation system consisting of all $(m-1) \cdot \binom{n}{2}$ instances of Eq. (4). Using the solver `fsolve` of MATLAB®'s optimization toolbox we then calculated all solutions to the system, i.e., the intersections of the curves, within a pre-defined area of interest.

To analyze the effect of the verifier's movement on the number of intersections within the area of interest, we define the verifiers' movements as depicted in Fig. 3. At the first $(i = 1)$ reception of the prover's claim, a verifier $\mathcal{V}_a$ is located at $\mathcal{V}_a^{(1)}$ and moves into direction α_a at a certain speed. As the prover re-transmits the location claim after Δ while the verifier moves at speed v into direction α_a, we can approximate the verifier's location at reception of the second transmission $(i = 2)$ by adding a vector of length $\Delta \cdot v$ and direction α_a to the initial location $\mathcal{V}_a^{(1)}$. It is worth noting that we set the verifier's location at the time of transmission equal to that of the reception time. While this is not realistic, we argue that this error is negligible in practice since the verifier's speed is extremely small compared to the signal propagation speed. For further transmissions $(i > 1)$ we consider only the direction change β_a, γ_a, and so on. In summary, a verifier's movement during the verification process can be completely described by its initial location $\mathcal{V}_a^{(1)}$, its speed v, the inter-transmission interval Δ, the initial direction α_a, and the direction changes β_a, γ_a, ... between the receptions.

6.2 Parameter Selection

To keep our simulations realistic, we have chosen the simulation parameters according to the stadium use case described in Section 2.4. The speed of the verifiers is assumed to be in the range of off-the-shelf drones (10-30 m/s). The



(a) Effect of step width/speed on the number of intersections. The gray solid line is the percentage of the cases in which the location was securely verified. The other lines represent the percentages where an adversary could have been located at an increasing number of locations other than $\mathcal{P}$.

(b) Effect of relative movement $(\alpha_a - \alpha_b)$ and different $\beta_a = \beta_b = \beta$ on the number of intersections. This graph only shows the percentage of the 10.000 random scenarios that were secure, i.e., the set of intersections $\mathcal{I}$ only contained $\mathcal{P}$.

Fig. 4. Simulation Results

distance covered between two transmissions of a location claim is the product of this speed and the inter-transmission interval Δ. For simplicity, we set $\Delta = 1$ s for all our simulations. The area of interest considered in our simulations is motivated by the size of a football stadium and set to a rectangle of 209x255 m. All verifiers and location claims must be within this area.

As for the adversary's location, we allow it to be located outside this area but limit its distance to the verifiers in the following way. We assume that each verifier has a circular reception range with a radius sufficient to cover the largest possible distance between two locations within the area of interest. As a consequence, if all verifiers are located at the same side of the area, an attacker located outside the area could still be in their coverage. We therefore extend the area in which we search for intersections with a safety margin of the length of the diagonal of the area of interest.

An example scenario matching this parameter selection would be a location-based service which should only be available to people within the stadium. To access the service without having to pay entry, the adversary tries to spoof a location within the stadium while being located outside (but in range). Drones are hovering in the stadium and act as verifiers.

6.3 Opportunistic/Random Mobility

Effect of speed v The speed of the verifiers defines the distance covered by a verifier between the periodic re-transmissions of a location claim. To evaluate whether the resulting step width has an impact on the number of intersections, we randomly generated 10.000 scenarios for the "cheapest" configuration $n = 2$ and $m = 3$. Each verifier starts at a random location $\mathcal{V}_{a/b}^{(1)}$ and moves into a random direction at different speeds $10 \leq v \leq 100$ m/s. For each scenario, we recorded the number of intersections $|\mathcal{I}|$. We did not consider larger speeds since they would be unrealistic given an area of interest of 209x255 m. The results are shown in Fig. 4a. While the percentage of scenarios in which the claimed location could be securely verified (gray solid line) slightly increased with increasing step width, the percentage of $|\mathcal{I}| = 2$ was constantly over 50%. For smaller v, there were even about 20% of scenarios in which an adversary could have chosen between two (dashed blue with squares) or three (green dashed with pluses) locations different to $\mathcal{P}$ which also satisfied Eq. (1) for both verifiers. We conclude that the step width (or speed) has only a minor effect on the number of intersections. On the one hand, this means that the step width does not provide much room for improving the security. However, on the other hand, this also means that slow verifiers do not suffer big disadvantages.

Effect of number of transmissions m and verifiers n Both numbers m and n affect the security by controlling the number of curves whose intersections define $\mathcal{I}$. As mentioned above, the adversary's location $\mathcal{A}$ must lie on $(m-1)\cdot\binom{n}{2}$ implicit curves in order to successfully spoof $\mathcal{P}$. As before, we start our analysis with the smallest configuration ($m = 3$ and $n = 2$) and generated 10.000 random verification scenarios with random initial verifier locations $\mathcal{V}_{a/b}^{(1)}$, random $\alpha_{a/b}$ and $\beta_{a/b}$, and random speeds $10 \leq v \leq 100$ m/s. As expected, the results were equal to those for the average step width of 55 m shown in Fig. 4a. Only 31.65% of all tested scenarios could be securely verified with the basic configuration of $m = 3$ and $n = 2$. A large number of scenarios resulted in two intersections (54.35%). The probability for more than two intersections, however, is significantly lower (less than 10% for three intersections). We conducted another 10.000 random simulations for $m = 4$ as well as for $n = 3$ and the number of intersections dropped to 1 for all tested scenarios, indicating that *our verification scheme is secure for $m > 3$ or $n > 2$.*

We can conclude that if the verifiers move opportunistically (random) within the area of interest, 31.65% of the location verification scenarios can be securely verified with $n = 2$ verifiers and $m = 3$ transmissions. In order to securely verify the other 68.35%, at least one additional transmission ($m > 3$) or at least one additional verifier ($n > 2$) is required. That means that if, for instance, the inter-transmission interval is $\Delta = 1$ s, an adversary would be discovered after 2 s in 31.65% of the scenarios and at latest after 3 s, resulting in an average verification time of 2.6835 s. Conversely, with an additional verifier, the verification time is reduced to 2 s.

6.4 Uncoordinated Controlled Mobility

The previous results show that our scheme is secure for $m > 3$ or $n > 2$. However, depending on the use case, reducing the verification time and minimum number of verifiers might be crucial. For example, if the area of interest is larger, parts of the area might only be covered by very few verifiers. In addition, message loss due to frequency overuse might reduce the number of messages received by a sufficient number of verifiers. To further increase the efficiency of our scheme for a better robustness against such problems, we now analyze whether the security of the minimum configuration ($m = 3$ and $n = 2$) improves if the verifiers' movements are controlled. Being able to securely verify a larger fraction of locations with the minimal configuration reduces the average verification time and the required number of verifiers.

Movement Pattern (α and β) Our next set of simulations aims at shedding light on the influence of the movement directions $\alpha_{a/b}$ and $\beta_{a/b}$ on $|\mathcal{I}|$. It is worth noting that we do not analyze the effect of the initial location $\mathcal{V}_{a/b}^{(1)}$ since we assume that the adversary controls the point in time when the verification process is initiated. Hence, the verifiers can only control what happens after the first location claim was received. In addition, we do not consider movement patterns as functions of $\mathcal{P}$ since this would prevent the verification of multiple positions at the same time.

For the following simulations, we set the speed of the verifiers to that of commercial off-the-shelf drones such as DJI's Phantom 4, i.e., $v = 20$ m/s. The turns of the verifiers between the two steps are controlled by β_a and β_b. To keep our scheme light-weight, we assume that the verifiers do not communicate for coordination and assume constant pre-defined $\beta_a = \beta_b = \beta$. However, since the curves determining $|\mathcal{I}|$ do not only depend on β but also on α_a and α_b, we further analyze how the difference between the two angles, i.e., the relative direction of the verifiers to each other affects the intersections. As before, we conducted 10.000 random simulations for different combinations of β and $\alpha_a - \alpha_b$.

The results are shown in Fig. 4b. The graph shows that both the effect of β and that of $\alpha_a - \alpha_b$ on $|\mathcal{I}|$ are almost independent from each other. Regardless of the difference in direction, any β close to $0°$ (respectively $360°$) should be avoided. For large direction differences $\alpha_a - \alpha_b$, the best choice for β is around $110°$ or $250°$. Note that both angles represent the same absolute change in direction since $360° - 250° = 110°$.

An interesting special case is $\beta = 180°$, i.e., the third location of each verifier is the same as the first one ($\mathcal{V}^{(1)} = \mathcal{V}^{(3)}$). As a result, the implicit curve generated by the first two transmissions coincides with that one of the second and third transmission. In other words, the third transmission does not impose a new constraint on the adversary and it is only limited to locations on the implicit curve (compare Section 4.2).

More specifically, let us assume two verifiers $\mathcal{V}_a$ and $\mathcal{V}_b$ receiving three transmissions of a location claim for $\mathcal{P}$. According to Sec. 4.2 a potential adversary's location $\mathcal{A}$ must satisfy the following system of instances of Eq. (4):

$$\begin{aligned}(\delta_{\mathcal{A},b}^{(2)} - \delta_{\mathcal{A},b}^{(1)}) &= (\delta_{\mathcal{A},a}^{(2)} - \delta_{\mathcal{A},a}^{(1)}) + k_{\mathcal{P}}^{(2)} \\ (\delta_{\mathcal{A},b}^{(3)} - \delta_{\mathcal{A},b}^{(2)}) &= (\delta_{\mathcal{A},a}^{(3)} - \delta_{\mathcal{A},a}^{(2)}) + k_{\mathcal{P}}^{(3)}\end{aligned}$$

If $\beta = 180°$, i.e, $\mathcal{V}_a^{(3)} = \mathcal{V}_a^{(1)}$ and $\mathcal{V}_b^{(3)} = \mathcal{V}_b^{(1)}$ then

$$\begin{aligned}k_{\mathcal{P}}^{(3)} &= (\delta_b^{(3)} - \delta_b^{(2)}) - (\delta_a^{(3)} - \delta_a^{(2)}) \\ &= (\delta_b^{(1)} - \delta_b^{(2)}) - (\delta_a^{(1)} - \delta_a^{(2)}) \\ &= -k_{\mathcal{P}}^{(2)}\end{aligned}$$

and thus

$$\begin{aligned} & (\delta_{\mathcal{A},b}^{(3)} - \delta_{\mathcal{A},b}^{(2)}) = (\delta_{\mathcal{A},a}^{(3)} - \delta_{\mathcal{A},a}^{(2)}) + k_{\mathcal{P}}^{(3)} \\ \Leftrightarrow \quad & (\delta_{\mathcal{A},b}^{(1)} - \delta_{\mathcal{A},b}^{(2)}) = (\delta_{\mathcal{A},a}^{(1)} - \delta_{\mathcal{A},a}^{(2)}) - k_{\mathcal{P}}^{(2)} \\ \Leftrightarrow \quad & (\delta_{\mathcal{A},b}^{(2)} - \delta_{\mathcal{A},b}^{(1)}) = (\delta_{\mathcal{A},a}^{(2)} - \delta_{\mathcal{A},a}^{(1)}) + k_{\mathcal{P}}^{(2)}\end{aligned}$$

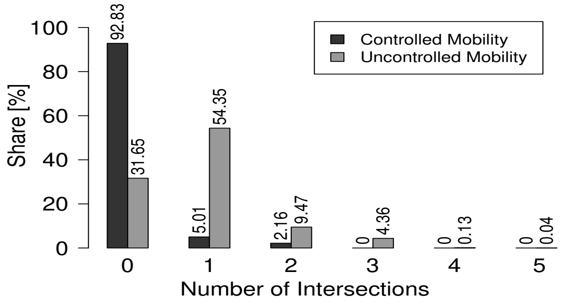


Fig. 5. Comparison of the distribution of the number of possible adversary positions for controlled and uncontrolled mobility ($n = 2$, $m = 3$). For controlled mobility we used $\alpha_a - \alpha_b = 180°$ and $\beta \approx 110°$.

Consequently, the third transmission does not impose a new constraint on the adversary's location $\mathcal{A}$ if $\beta = 180°$.

Regarding the direction difference $\alpha_a - \alpha_b$, we can summarize that the closer it is to $180°$, the higher the percentage of locations which could be securely verified after the third transmission. In fact, we also did the simulations for $\alpha_a - \alpha_b > 180°$ but the results were identical to those for $360° - (\alpha_a - \alpha_b)$.

We conclude from our simulations that with $\beta = 110°$ or $\beta = 250°$ and a direction difference of $|\alpha_a - \alpha_b| = 180°$, more than 92.5% of all scenarios could be securely verified with two verifiers and three transmissions of the location claim. This is a huge improvement compared to random movement as shown in Fig. 5.

7 Related Work

As already mentioned in the introduction, many solutions and methods have been proposed in the literature to solve the problem of secure location verification. Existing solutions can broadly be classified into methods based on distance bounding [2, 12, 19, 15, 20], time-difference of arrival measurements (TDoA) [19, 22, 16], angle of arrival measurements [6, 8], or hybrid methods [4, 3]. As mentioned in the introduction, each of these schemes comes with limiting requirements such as tight time synchronization, specialized hardware, directional antennas, or limited attacker knowledge. We therefore argue that they are not applicable to scenarios where passive and lightweight solutions are required.

Only a few works have tackled the case of mobile verifiers for secure location verification. However, these protocols differ significantly from ours. Čapkun et al. [21] proposed a location verification scheme, in which a mobile verifier initiates a challenge-response protocol from a known position and then moves to an unknown position to receive the response. The response is sent simultaneously via ultrasound and RF so that the verifier can estimate its distance to the prover based on the time-difference of arrival of the two signals due to their differing propagation speed (ranging). The security of the approach derives from the fact that although dishonest provers could modify the transmission times of the two response signals, they would need to correctly guess the verifier's new location in order to mimic the expected time-difference of arrival. This scheme, however, is cooperative and requires nodes to be equipped with two transceivers (ultrasound and RF). Moreover, we challenge the assumption 'untraceability' of the moving verifier. Even though the verifier does not actively transmit revealing signals from its new location, a more sophisticated adversary could track the verifier via reflections of signals of opportunity and passive radar techniques [5].

In [10], Perazzo et al. propose a location verification system in which a verifier drone performs distance bounding with a prover consecutively from several different locations. The locations are carefully chosen such that they form a triangle containing the prover's location. In this way an adversary claiming a false location inside the triangle needs to mimic a shorter distance to at least one of the locations chosen by the drone. As shown by Čapkun et al. in [20], this is infeasible and hence, the scheme is secure. However, their approach inherits all the aforementioned system requirements from distance bounding and is therefore not well-suited for location verification in existing systems or systems with limited resources.

Baker and Martinovic proposed a TDoA-based scheme in [1]. Their scheme relies on two verifiers, one fixed and the other one moving, to measure the TDoA of multiple location broadcasts by the prover. Since one verifier is changing location between each of the prover's transmissions, different TDoAs are expected each time. Analogously to traditional multilateration, each TDoA measurement reduces the set of possible locations of the transmitter to one arm of a hyperbola. By repeating the measurements at least three times (in 2D) and comparing the expected to the measured TDoAs, the adversary can be localized by intersecting the resulting hyperbolas. As mentioned, however, TDoA measurements require tight time synchronization and extra communication to collect all measurements at a central processing unit which our protocol does not require.

Finally, we want to highlight the difference of this work to our related works on track verification [13] and motion verification [14]. First, the underlying problem considered in this paper (verification of locations) is different to that considered in [13] (verification of sequences of locations) or [14] (verification of motion). The seemingly strong similarity is largely a result of the common theoretical foundations on which these works are based on. This work, however, diverges significantly in terms of problem statement, use cases, and security properties from our previous works. More specifically, the theoretical analysis conducted in this paper considers multiple moving nodes at the same time, whereas the analyses of [13] and [14] are only applicable to systems with one moving node. As a result, the analytical nature of the security guarantees of our scheme is not hyperbolic anymore, making them much harder to analyze.

8 Conclusion

In this paper, we presented *MoVers*, a simple yet secure location verification method which leverages the mobility of verifiers to relax system requirements. We have provided a formal security analysis which shows that our scheme MoVers achieves provable security with only two transmissions by adjusting the movements of two verifiers to the claimed location. We have furthermore shown in simulations how more general types of mobility affect the security of our scheme.

References

1. Baker, R., Martinovic, I.: Secure location verification with a mobile receiver. In: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC) (Oct 2016)
2. Brands, S., Chaum, D.: Distance-bounding protocols. In: Advances in Cryptology, vol. 765. Springer Berlin Heidelberg, workshop on the theory and application of cryptographic techniques (eurocrypt '93) edn. (1994)
3. Chiang, J.T., Haas, J.J., Choi, J., Hu, Y.C.: Secure location verification using simultaneous multilateration. IEEE Transactions on Wireless Communications **11**(2) (Feb 2012)
4. Chiang, J.T., Haas, J.J., Hu, Y.C.: Secure and precise location verification using distance bounding and simultaneous multilateration. In: Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec) (Mar 2009)
5. Howland, P.: Editorial: Passive radar systems. IEE Proceedings - Radar, Sonar and Navigation **152**(3), 105–106 (June 2005). https://doi.org/10.1049/ip-rsn:20059064
6. Hu, L., Evans, D.: Using Directional Antennas to Prevent Wormhole Attacks . In: Network and Distributed System Security Symposium (NDSS) (Feb 2004)
7. International Civil Aviation Organization (ICAO): International Standards and Recommended Practices, Annex 10: Aeronautical Telecommunications, 6 edn. (2006), Volume I: Radio Navigation Aids
8. Lazos, L., Poovendran, R., Čapkun, S.: ROPE: Robust Position Estimation in Wireless Sensor Networks. In: Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN). IEEE Press (Apr 2005)
9. Li, H., Hestenes, D., Rockwood, A.: Generalized Homogeneous Coordinates for Computational Geometry. Springer Verlag (2001)
10. Perazzo, P., Ariyapala, K., Conti, M., Dini, G.: The verifier bee: A path planner for drone-based secure location verification. In: Proceedings of the 16th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) (June 2015)
11. Rasmussen, K.B., Čapkun, S.: Realization of rf distance bounding. In: Proceedings of the 19th USENIX Conference on Security (2010)
12. Sastry, N., Shankar, U., Wagner, D.: Secure verification of location claims. In: Proceedings of the 2nd ACM Workshop on Wireless Security (WiSe) (Sep 2003)
13. Schäfer, M., Lenders, V., Schmitt, J.B.: Secure track verification. In: IEEE Symposium on Security and Privacy (May 2015)
14. Schäfer, M., Leu, P., Lenders, V., Schmitt, J.: Secure motion verification using the doppler effect. In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec) (Jul 2016)
15. Singelee, D., Preneel, B.: Location verification using secure distance bounding protocols. In: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference (MASS) (Nov 2005)
16. Strohmeier, M., Lenders, V., Martinovic, I.: Lightweight location verification in air traffic surveillance networks. In: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security (CPSS) (2015)
17. Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., Martinovic, I.: On perception and reality in wireless air traffic communication security. IEEE Transactions on Intelligent Transportation Systems **18**(6) (Jun 2017)
18. Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B., Capkun, S.: On the requirements for successful gps spoofing attacks. In: Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS) (Oct 2011)

19. Čapkun, S., Hubaux, J.P.: Securing position and distance verification in wireless networks. Tech. rep., École polytechnique fédérale de Lausanne (EPFL) (2004)
20. Čapkun, S., Hubaux, J.P.: Secure positioning of wireless devices with application to sensor networks. In: Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM). vol. 3 (Mar 2005)
21. Čapkun, S., Rasmussen, K.B., Čagalj, M., Srivastava, M.: Secure location verification with hidden and mobile base stations. IEEE Transactions on Mobile Computing **7**(4) (Apr 2008)
22. Čapkun, S., Čagalj, M., Srivastava, M.: Secure localization with hidden and mobile base stations. In: Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM) (Apr 2006)