POSTER: Secure Path Verification using Mobility-Differentiated ToA

Matthias Schäfer
TU Kaiserslautern
Germany
schaefer@cs.uni-kl.de

Vincent Lenders
armasuisse
Switzerland
vincent.lenders@armasuisse.ch

Jens Schmitt
TU Kaiserslautern
Germany
jschmitt@cs.uni-kl.de

ABSTRACT

In this poster, we generalize the problem of secure location verification to that of *path* verification and propose a scheme to securely verify the claims of a mobile node that moves along a path. Although the secure verification of location claims has been studied extensively in the literature, current solutions require very strict time synchronization of the verifiers, or extra communication and special-purpose hardware. However, we propose a lightweight verification scheme exploiting the mobility of the claimer in path verification without need for time synchronization and communication overhead.

1. INTRODUCTION

In location verification, a set of so-called *verifiers* wish to verify whether a *prover* is in a region (or at a position) of interest [3]. Many schemes have been proposed in the past decade to solve this problem [5]. There are active schemes which employ specialized protocols to derive upper bounds on the distance to the prover. On the other hand, passive methods (e.g. multilateration, radar) allow verification by using information such as time differences or angles of signal arrivals. However, both approaches suffer from costly requirements which cannot always be assumed in existing systems. For instance, active schemes are only applicable if the prover is equipped with spezialized hardware and passive methods require tightly synchronized verifiers to measure propagation time differences of the prover's signal.

In this poster, we present a novel scheme based on the mobility-differentiated time of arrival. It exploits the mobility of the prover to verify its position securely while relaxing the system requirements of the verification significantly. In particular, our scheme does not require verifiers to be synchronized, nor does it require any additional communication between prover and verifiers.

The lightweight nature of our scheme makes it particularly suitable for the verification of trajectories in air and maritime transportation systems as well as vehicular networks which require continuous tracking of vehicles or aircraft. Previous research has pointed out that the existing systems in this area are particularly vulnerable to location spoofing attacks [1, 4] and require lightweight solutions that can be deployed gradually without costly and long-lasting system upgrades of the current infrastructure.

2. SECURE PATH VERIFICATION

Analogously to secure *location* verification from Sastry et al. in [3], we define the problem of secure *path* verification as follows. A set of verifiers V wish to verify whether a prover moves on a path P. The path claim consists of at least two location claims, i.e. $P = \{C_1, \dots, C_n\}$ with $n \geq 2$. Each location claim C_i is a tuple $(\bar{t}_i, \vec{p}_i)$ where $\bar{t}_i$ denotes a prover-local timestamp with its corresponding location $\vec{p}_i$. The location claim C_i is sent at time $\bar{t}_i$ and from location $\vec{p}_i$. We require that $\vec{p}_i \neq \vec{p}_j$ holds for at least one pair $i, j \leq n$. Otherwise, the problem would be identical to [3].

2.1 Assumptions & Notation

We assume that both, prover and verifiers are equipped with clocks which are not necessarily synchronized. Timestamps represent the local time of a node at a certain event. To distinguish between global time and local timestamps, we denote global time with t and the node-local time that corresponds to t (i.e. the timestamp at time t) with $\bar{t}$. For now we assume that all clocks have the same speed, i.e. clock drift is ignored. We discuss the effect of clock drift later on.

The timespan between two location claims C_i and C_j is denoted by $\Delta_{i,j} = t_j - t_i$. Note that for valid location claims $\Delta_{i,j} = \bar{t}_j - \bar{t}_i$ holds as well. The time of arrival of a location claim C_i at verifier $V_x \in V$ is denoted by t_i^x. Analogously, the timespan between the arrivals of two location claims C_i and C_j at V_x is denoted by $\Delta_{i,j}^x = t_j^x - t_i^x$. The propagation delay of C_i's signal on its way to verifier V_x is denoted with $\Delta_i^x = t_i^x - t_i$. Hence,

$$\Delta_{i,j}^x = \Delta_{i,j} + (\Delta_j^x - \Delta_i^x) \tag{1}$$

2.2 Basic Scheme

A prover sends location claims C_i to a set of stationary verifiers $\{V_x, V_y, \dots\}$ using a wireless communication channel. We assume that there is no compromised verifier and all verifiers are able to communicate securely with each other. Each verifier V_x knows its position $\vec{p}_x$. Then for all $C_i, C_j \in P$ with $i \neq j$, each verifier checks the following equation:

$$\overline{\Delta}_{i,j}^x \stackrel{?}{=} \overline{\Delta}_{i,j} + (\Delta_j^x - \Delta_i^x) \tag{2}$$

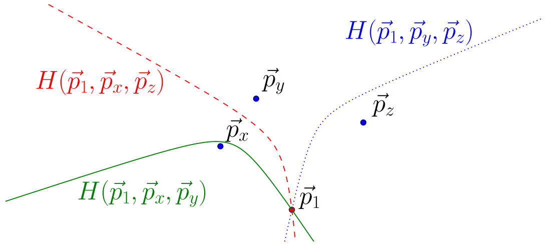
$H(\vec{p}_1, \vec{p}_y, \vec{p}_z)$
$H(\vec{p}_1, \vec{p}_x, \vec{p}_z)$
$\vec{p}_y$
$\vec{p}_z$
$\vec{p}_x$
$H(\vec{p}_1, \vec{p}_x, \vec{p}_y)$
$\vec{p}_1$

Figure 1: Example with three verifiers.

where the propagation delay $\Delta^x_{i/j}$ is estimated using $\vec{p}_x$, $\vec{p}_{i/j}$, and the propagation speed of $C_{i/j}$'s signal. After this evaluation phase, the verifiers exchange their results. Finally, an attack is detected if Equation 2 is violated at any of the verifiers.

It is important to note that clocks are not required to be synchronized in Equation 2. We only consider timespans which can be computed from the local timestamps provided by the location claims and time of arrival measurements. This is comparable to mobility-differentiated time of arrival (MDToA) proposed in [2] for self-localization using location beacons sent from a mobile node.

It is worth noting that the assumptions made by this scheme are fully compliant with the conditions given in real systems, for instance, in the automatic dependent surveillance–broadcast (ADS-B) protocol used in the next generation air transportation system. Here, airplanes report their positions periodically to nearby stationary ground stations. These stations could therefore use our scheme to check reported trajectories of aircraft for consistency.

2.3 Attacker Model

We assume a stationary adversary A at position $\vec{p}_A$. The adversary uses an omni-directional antenna, i.e. all verifiers receive the same location claims. However, the adversary has full control of the location claim's content. In particular, $\vec{p}_i$ and $\overline{t}_i$ can be set to arbitrary values and the transmission time t_i of C_i is not necessarily correlated with the timestamp $\overline{t}_i$. In addition to these assumptions, the adversary knows the exact position of all verifiers in V.

2.4 Security Analysis

For convenience, we only consider the two-dimensional case. Extending our results to three dimensions is straightforward. We can show that the attacker can easily spoof arbitrary paths for a single verifier ($|V| = 1$) by adjusting the transmission times t_i accordingly. Yet, increasing the number of verifiers reduces the attacker's degree of freedom significantly.

The intuition behind this is as follows. As the prover is changing its position between individual location claims, the propagation delay to each verifier also must change in order to satisfy Equation 2 at all verifiers. Thus, adversaries would have to vary the propagation delays to each of the verifiers independently to successfully pretend movement. As a result, the only spoofable path for a stationary adversary is the path where the difference in propagation delay to each verifier is constant. For two verifiers, this is a hyperbola. For more than two verifiers, this property only holds for the intersections of the pairwise hyperbolas (see Figure 1).

Our theoretical analysis confirms that with $|V| = 2$, the attacker can only spoof paths along a hyperbola. Any spoofed path different from this hyperbola would result in a violation of Equation 2 at one of the receivers.

We generalized this result for more than two verifiers by considering the pairwise hyperbolas and their intersections. For three verifiers, there is either no (Figure 1) or at most one further intersection besides the first claimed position. This means that with three verifiers, the attacker cannot spoof any path P with $|P| > 2$. Although this is already good enough for most applications, a unique solution can be guaranteed if the node distribution ensures that each position is covered by at least four verifiers.

2.5 Dealing With Noise

In practice, verifiers have to deal with erroneous values. For example, clocks have different speeds which results in clock drifts (i.e. $\overline{\Delta_{i,j}} \neq \Delta_{i,j}$). The noise due to clock drift, ϵ_{drift} is linearly dependent on $\Delta^x_{i,j}$. Furthermore, our scheme is based on precise time of arrival measurements. However, time of arrival measurements always involve noise in practice. We assume this noise to be zero-mean Gaussian. Its variance depends on the clock speed of the verifiers' clocks. Combining these two sources of noise, we can model the error due to noise as $\epsilon \sim \mathcal{N}(\epsilon_{drift}, \sigma^2)$. Therefore, our verification scheme needs to be extended with respect to this error. Instead of considering a Boolean decision variable based on Equation 2, an attack is detected, if the likelihood

$$P_{\mathcal{N}(\epsilon_{drift},\sigma^2)}(\epsilon = \overline{\Delta}^x_{i,j} - \overline{\Delta}_{i,j} - (\Delta^x_j - \Delta^x_i)) \tag{3}$$

drops below a certain threshold at one verifier. This threshold can be tuned according to a desired tolerance level for the false positive and false negative rates.

3. CONCLUCION

In this poster, we present a scheme for verifying a path a mobile node, such as a car or an aircraft, claims to move on. We present our basic scheme that exploits the prover's mobility to avoid the need for synchronization and additional communication. We discuss its security as well as its practicability.

4. REFERENCES

[1] Andrei Costin and Aurélien Francillon. Ghost is in the Air(traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Black Hat USA, July 2012. White paper.

[2] J. Luo, H. V. Shukla, and J.-P. Hubaux. Non-interactive location surveying for sensor networks with mobility-differentiated toa. In *International Conference on Computer Communications*, INFOCOM. IEEE, April 2006.

[3] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Workshop on Wireless Security*, WiSe. ACM, 2003.

[4] M. Schäfer, V. Lenders, and I. Martinovic. Experimental analysis of attacks on next generation air traffic communication. In *Applied Cryptography and Network Security*, ACNS. Springer, June 2013.

[5] Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie. Secure localization and location verification in wireless sensor networks: a survey. *The Journal of Supercomputing*, 64(3), 2013. Springer.