On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer  
Dept. of Computer Science  
ETH Zurich, Switzerland  
tinils@inf.ethz.ch

Christina Pöpper  
Dept. of Computer Science  
ETH Zurich, Switzerland  
poepperc@inf.ethz.ch

Kasper B. Rasmussen  
Computer Science Dept.  
UCI, Irvine, CA  
kbrasmus@ics.uci.edu

Srdjan Ćapkun  
Dept. of Computer Science  
ETH Zurich, Switzerland  
capkuns@inf.ethz.ch

ABSTRACT
An increasing number of wireless applications rely on GPS signals for localization, navigation, and time synchronization. However, civilian GPS signals are known to be susceptible to spoofing attacks which make GPS receivers in range believe that they reside at locations different than their real physical locations. In this paper, we investigate the requirements for successful GPS spoofing attacks on individuals and groups of victims with civilian or military GPS receivers. In particular, we are interested in identifying from which locations and with which precision the attacker needs to generate its signals in order to successfully spoof the receivers.

We will show, for example, that any number of receivers can easily be spoofed to one arbitrary location; however, the attacker is restricted to only few transmission locations when spoofing a group of receivers while preserving their constellation.

In addition, we investigate the practical aspects of a satellite-lock takeover, in which a victim receives spoofed signals after first being locked on to legitimate GPS signals. Using a civilian GPS signal generator, we perform a set of experiments and find the minimal precision of the attacker’s spoofing signals required for covert satellite-lock takeover.

Categories and Subject Descriptors
C.2.1 [Computer Systems Organization]: Computer-Communication Networks—Network Architecture and Design

General Terms
Security, Experimentation

1. INTRODUCTION
The Global Positioning System (GPS), originally introduced by the US military, has become an essential component for numerous civilian applications. Unlike military GPS signals, civilian GPS signals are not encrypted or authenticated and were never intended for safety- and security-critical applications. Nevertheless, GPS-provided locations are being used in applications such as vehicular navigation and aviation, asset monitoring (e.g., cargo tracking), and location-based services (e.g., routing) [23]. The use of the GPS system also includes time synchronization; examples are time stamping in security videos and critical time synchronization in financial, telecommunications and computer networks. Users highly rely on the precision and correctness of GPS location and time: transport companies track trucks, cargoes, and goods under GPS surveillance, and courts rely on criminals being correctly tracked by GPS-based ankle monitors.

This heavy reliance on civilian GPS—following the discontinuation of the selective availability feature of GPS in the year 2000—motivated a number of investigations on the security of GPS. These investigations found that civilian GPS is susceptible to jamming and spoofing attacks [9, 11, 16, 19]. Successful spoofing experiments on standard receivers have been reported [7, 24], showing that commercial-off-the-shelf receivers do not detect such attacks.

The increased availability of programmable radio platforms such as USRPs [5] leads to a reduced cost of attacks on GPS. However, the requirements for GPS spoofing were so far not analyzed systematically and many of the previously proposed countermeasures [8, 16] assume a weak attacker that is, e.g., not able to generate signals with sufficient precision.

In this work, we investigate spoofing attacks on civilian and military GPS and analyze the requirements for their success as well as their limitations in practice. We divide the problem of GPS spoofing into the following two problems: (i) sending the correct spoofing signals such that they reach the receiver with the right timing, and (ii) getting a victim that is already synchronized to the legitimate GPS service to lock onto the attacker’s spoofing signal. Regarding the first problem, we analyze the effects of GPS spoofing signals on multiple receivers and analyze under which conditions a group of victims can be spoofed such that, e.g., their mutual distances are preserved. Our analysis shows that, in order to spoof a group of victims while preserving the mutual distances, the attacker can only transmit from a restricted set of locations. To the best of our knowledge, such an analysis has not been done before. The second problem of taking over the satellite lock is relevant for performing attacks in real-world situations. In most cases, the victim will have been receiving legitimate GPS signals when the spoofing attack starts. It is thus important to know the required precision of the spoofing signal such that the victim seamlessly (i.e., without detection) switches lock from the legitimate GPS signal to the attacker’s spoofing signal. We explore the influence of imperfections (in different aspects of signal power and timing) in a series of experiments and discuss the findings.

The structure of the paper is as follows. We give background information on GPS positioning and discuss related work on GPS spoofing in Section 2. We introduce the GPS spoofing problem and our system and attacker models in Section 3. In Section 4,
we analyze under which conditions GPS spoofing attacks are successful on single victims and groups of victims. The results of our experimental evaluation are presented in Section 5. In Section 6, we introduce a novel countermeasure which is based on multiple receivers. We conclude the paper in Section 7.

2. BACKGROUND

In this section, we introduce the fundamental concepts of GPS (based on [11]) which are necessary for this work. We also summarize related work on the security of GPS.

2.1 The Global Positioning System

The Global Positioning System (GPS) uses a number of satellite transmitters \( S_i \) located at known locations \( L_{S_i} \in \mathbb{R}^3 \). Each transmitter is equipped with a synchronized clock with no clock offset to the exact system time \( t^S \) and broadcasts a carefully chosen navigation signal \( s_i(t) \) (low auto-cross-correlation\(^1\), including timestamps and information on the satellites’ deviation from the predicted trajectories). The signal propagates with speed \( c \) (see Figure 1).

A receiver \( V \) located at the coordinates \( L \in \mathbb{R}^3 \) (to be determined) and using an omnidirectional antenna will receive the combined signal of all satellites in range:

\[
g(L, t) = \sum_i A_i s_i \left( t - \frac{|L_{S_i} - L|}{c} \right) + n(L, t) \quad (1)
\]

where \( A_i \) is the attenuation that the signal suffers on its way from \( L_{S_i} \) to \( L \), \( |L_{S_i} - L| \) denotes the Euclidean distance between \( L_{S_i} \) and \( L \), and \( n(L, t) \) is background noise.

Due to the properties of the signals \( s_i(t) \), the receiver can separate the individual terms of this sum and extract the relative spreading code phase, satellite ID, and data content using a replica of the used spreading code. Given the data and relative phase offsets, the receiver can identify the time delay \( |L_{S_i} - L|/c \) for each satellite and from that infer the “ranges”

\[
d_i = |L_{S_i} - L|. \quad (2)
\]

With three known ranges \( d_i \) to known transmitter positions \( L_{S_i} \), three equations (2) can be solved unambiguously for \( L \) (unless all three \( S_i \) are located on a line). Since highly stable clocks (e.g., cesium oscillators) are costly and GPS receivers cannot participate in two-way clock synchronization, in practice, \( V \) will have a clock offset \( \delta \) to the exact system time: \( t = t^S + \delta \). With this, Eq. 1 can be rewritten:

\[
g(L, t^S) = \sum_i A_i s_i \left( t - d_i/c - \delta \right) + n(L, t^S) \quad (3)
\]

where the receiver can only infer the “pseudoranges” \( R_i \) from the delays \( d_i/c + \delta \):

\[
R_i = d_i + c \cdot \delta. \quad (4)
\]

The clock offset \( \delta \) adds a fourth unknown scalar. With pseudorange measurements to at least four transmitters \( S_i \), the resulting system of equations (4) can be solved for both \( L \) and \( \delta \), providing both the exact position and time, without requiring a precise local clock. Given \( L_{S_i} = (x_{S_i}, y_{S_i}, z_{S_i}) \), \( L = (x, y, z) \), and \( \Delta = c \cdot \delta \), we can transform (4) into the following set of equations [1]:

\[
(x - x_{S_i})^2 + (y - y_{S_i})^2 + (z - z_{S_i})^2 = (R_i - \Delta)^2 \quad \forall S_i \quad (5)
\]

\(^1\)In civilian GPS, the signals are spread using publicly known spreading codes. The codes used for military GPS are kept secret; they serve for signal hiding and authentication.

![Figure 1: A GPS receiver \( V \) works by observing the signals from a set of satellites. The relative delays of the signals \( s_i(t) \) can be used to solve four equations which determine the 3-dimensional position \( L \) and the time offset \( \delta \) of the receiver \( V \).](image-url)

Geometrically, given a \( \Delta \), each \( S_i \)’s equation translates into a sphere with \( L_{S_i} \) being the center. The set of equations (5) is overdetermined for more than four satellites and generally does not have a unique solution for \( L \) because of data noise. It can be solved by numerical methods such as a least-mean-square approach or Newton’s method [1].

2.2 Related Work

In 2001, the Volpe report [8] identified that (malicious) interference with the civilian GPS signal is a serious problem. Starting with this report, practical spoofing attacks were discussed in several publications. In [24], the authors use a WelNavigate GS720 satellite simulator mounted in a truck to attack a target receiver in a second truck. The authors succeeded in taking over the victim’s satellite lock by manually placing an antenna close to the victim’s receiver. After the victim was locked onto the attacker’s signal the spoofing signal could be sent from a larger distance. Instead of using a GPS simulator, the authors of [7] create GPS spoofing signals by decoding legitimate GPS signals and generating time-shifted copies which are then transmitted with higher energy to overshadow the original signals; a similar approach is also used in [14]. This approach requires less expensive equipment but introduces considerable delays between the legitimate and the spoofed signals. GPS spoofing attacks are discussed analytically in [11], showing that an attacker can manipulate the arrival times of military and civilian GPS signals by pulse-delaying or replaying (individual) navigation signals with a delay. We note that there is no unique attacker model used for spoofing attacks, and thus the assumptions on the attacker’s capabilities vary between these works.

Given the lack of attacker models, the proposed countermeasures range from simple measures to constant monitoring of the channel. In [8], consistency checks based on inertial sensors, cryptographic authentication, and discrimination based on signal strength, time-of-arrival, polarization, and angle-of-arrival are proposed. The authors of [16, 17, 25] propose countermeasures based on detecting the side effects of a (not seamless) hostile satellite-lock takeover, e.g., by monitoring the local clock and Doppler shift of the signals. Kuhn proposes an asymmetric scheme in [11], based on the delayed disclosure of the spreading code and timing information. In general, countermeasures that rely on modifications of the GPS satellite signals or the infrastructure (such as [11] and certain proposals in [8]) are unlikely to be implemented in the near future due to long procurement and deployment cycles. At the same time, countermeasures based on lock interrupts or signal jumps do not detect seamless satellite-lock takeovers.

Few publications [3, 12–14] present experimental data on the effects seen by the victim during a spoofing attack. The authors
of [13] use a setup based on two antennas to measure the phase difference for each satellite to detect the lock takeover. [3] and [14] analyze the spoofing effect on the carrier and code level. The authors of [12] present a device that prevents spoofing by monitoring and potentially suppressing the received signals before they are processed by the GPS receiver.

All works above only consider attacks on single GPS receivers but not on groups of receivers. In addition, none of them investigated the requirements for successful attacks on public GPS receivers, such as required precision of the attacker’s spoofing signals. Although we expect that more works on GPS spoofing and anti-spoofing countermeasures were performed in classified (military) settings, they are not accessible to the public.

3. PROBLEM FORMULATION

In order to give an intuition of the problem, we present our motivation and an exemplary use case. Then, we define our system and attacker models and formulate the GPS spoofing problem.

3.1 Motivation

The fundamental reasons why GPS spoofing works have been discussed in the literature before, and spoofing attacks have been demonstrated on single receivers experimentally. In this work, we show under which conditions the attacker can establish the correct parameters to launch a successful spoofing attack on one or more victims, and later in the experiments, how inaccuracies in these parameters influence the lock takeover during the attack. This analysis enables us to identify which attacks are theoretically possible and which attacks would be noticeable as (potentially non-malicious) signal loss at the GPS receivers. This is important for proposing effective receiver-based countermeasures, which are not implemented yet in current standard GPS receivers.

Our work is further motivated by the real-life spoofing attacks, e.g. the one reported in [24]. In this scenario, a cargo truck (the victim) had a GPS unit that was housed in a tamper-proof casing and was sending cryptographically authenticated status updates with a fixed rate to a monitoring center. The attacker planned to steal the truck to get access to its loaded goods at a remote place. He got close to the victim and started transmitting forged (spoofed) signals in order to modify the location computed by the receiver (see Figure 2). In this setting, if the attacker can influence the localization process, he can make the victim report any position to the monitoring center and thus steal the truck without raising suspicion or revealing the truck’s real location.

3.2 System Model

Our system consists of a set of legitimate GPS satellites and a set $\mathcal{V}$ of victims (see Table 1 for notations used). Each victim is equipped with a GPS receiver that can compute the current position and time as described in Section 2. We assume that each receiver $V_j \in \mathcal{V}$ is able to receive wireless GPS signals, compute its position, and store its position/time-tuples. If several GPS receivers belong to a common group (e.g., they are mounted on the same vehicle), we assume that they can communicate and exchange their computed locations or are aware of the group’s (fixed) formation.

The GPS location of each individual victim $V_j \in \mathcal{V}$ is given by its coordinates $L_j \in \mathbb{R}^3$ and the victim’s clock offset $\delta_j$ with respect to the GPS system time $t^S$. We note that the computed GPS coordinates $L_j$ and clock offset $\delta_j$ do not necessarily correspond to the true (physical) coordinates $P_j \in \mathbb{R}^3$ and time. We define the local time of $V_j$ as $t_j = t^S + \delta_j$, i.e., $\delta_j < 0$ refers to an internal clock that lags behind. We use $\mathcal{L}$ to denote the set of GPS locations of the victims in $\mathcal{V}$. A GPS spoofing attack may manipulate a receiver’s coordinates in space and/or its local time. We denote a victim’s spoofed coordinates by $L_j' \in \mathbb{R}^3$ and the spoofed time offset by $\delta_j'$. We use $\mathcal{L}'$ for the set of spoofed victim locations.

In our analysis in Section 4, we distinguish between civilian GPS, which uses the public C/A codes so that each satellite signal contains only public information, and military GPS, which provides authentic, confidential signals using the secret P(Y) codes. In the experimental evaluation in Section 5, we use a satellite signal generator for civilian GPS.

3.3 Attacker Model

GPS signals can be trivially spoofed under a Dolev-Yao [4]-like attacker that is able to fully control the wireless traffic by intercepting, injecting, modifying, replaying, delaying, and blocking messages without temporal constraints for individual receivers, see Figure 3(b). If the attacker has full control over the input to each individual receiver antenna, he can send the signals as they would be received at any location $L_j'$. This would, however, require the attacker to either be very close to each receiver or to use directional antennas with narrow beam widths and shielding to prevent that the signals intended for one victim are also received by another victim; in both cases, the number of required attacker antennas would be linear in the number of victims. In this work we assume that the signals sent by the attacker are transmitted wirelessly and that they will be received by all victims in $\mathcal{V}$, see Figure 3(a).

The attacker controls a set of wireless transmitters that he can move and position independently. We denote by $P^A_i \in \mathbb{R}^3$ the

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_i$</td>
<td>$i$-th satellite</td>
</tr>
<tr>
<td>$L_i^S$</td>
<td>coordinates of $S_i$</td>
</tr>
<tr>
<td>$s_i$</td>
<td>signal sent by $S_i$</td>
</tr>
<tr>
<td>$v_j$</td>
<td>$j$-th victim (receiver)</td>
</tr>
<tr>
<td>$L_j$</td>
<td>GPS coordinates of $v_j$</td>
</tr>
<tr>
<td>$L'_j$</td>
<td>spoofed coordinates of $v_j$</td>
</tr>
<tr>
<td>$P^A_i$</td>
<td>physical coordinates of $A_i$</td>
</tr>
<tr>
<td>$s^A_i$</td>
<td>signal sent by $A_i$</td>
</tr>
<tr>
<td>$A_i$</td>
<td>$i$-th attacker unit</td>
</tr>
<tr>
<td>$\delta_i$</td>
<td>time offset of $s^A_i$</td>
</tr>
<tr>
<td>$\delta_i'$</td>
<td>spoofed clock offset of $v_j$</td>
</tr>
<tr>
<td>$\mathcal{L}$</td>
<td>set of legitimate GPS satellites</td>
</tr>
<tr>
<td>$\mathcal{V}$</td>
<td>set of victims</td>
</tr>
<tr>
<td>$t^S$</td>
<td>GPS clock offset of $v_j$</td>
</tr>
<tr>
<td>$c$</td>
<td>signal propagation speed</td>
</tr>
</tbody>
</table>

\[ \Delta_j' = \delta_j' \cdot c \]

Typically, the difference $|L - P|$ is less than a few meters [22].
spoofing problems for the attacker. In a GPS spoofing attack, the attacker sends spoofing signals to manipulate the victim’s GPS-based location calculations. As a result, $V$ computes its location as $L' \neq L$ and/or time as $t' \neq t$.

Definition 1 can also be extended to groups of victims:

**Definition 2 (GPS Group Spoofing Problem).** Let $L'$ be a set of target locations for each $V_i \in V$ and let $t'_i \in T'$ denote the target time for $V_i$. The GPS Group Spoofing Problem is the problem of using combinations of GPS signals $s_i^A$ (sent by the attacker), transmission times $t_i^A = t_i^S + \delta_i^A$ (when the spoofing signals are sent), and physical transmission locations $P_i^A$ (from where the attacker transmits) such that the location or time of each $V_i \in V$ is spoofed according to Definition 1.

We note that the physical attacker locations $P_i^A$ do not have to correspond to the claimed satellite positions $L_i^A$ in the GPS messages (for civilian GPS, $L_i^A$ can even be chosen by the attacker). As we will show in Section 4.2, the GPS spoofing problem for a single victim has a trivial solution for any target location.

In Section 4.3, we will analyze the necessary restrictions on the spoofed locations such that the GPS Group Spoofing Problem can be solved. We therefore define a decisional version of the GPS Group Spoofing Problem.

**Definition 3 (Decisional GPS Group Spoofing Problem).** Let $P$ be the set of physical locations of the victims in $V$. Let $L'$ and $T'$ be defined according to Definition 2. The Decisional GPS Group Spoofing Problem for $P, L', T'$ is the decision problem whether there exists at least one set of attacker locations $P^A$ from where the attacker can send the spoofing signals $s_i^A$ such that the location or time of each victim $V_i \in V$ is spoofed according to Definition 1.

In practice, the GPS Group Spoofing Problems (Definitions 2 and 3) may be restricted in terms of attacker capabilities. For example, the attacker may only be able to position his transmission antennas at a restricted set of physical locations $P^A$, at a restricted set of claimed satellite positions $L^A$, or he may only be able to send the spoofing signals at a restricted set of transmission times $T^A$ (e.g., if he must receive legitimate signals before he can send the spoofing signals). In these cases, the GPS Group Spoofing Problems can be modified to take the restricted attacker capabilities $L^A, P^A, T^A$ as additional input and find solutions that fulfill $P^A \subset P^A, L^A \subset L^A, T^A \subset T^A$.

4. SOLVING GPS SPOOFING PROBLEMS

We now analyze how our attacker (as defined in Section 3.3) can spoof the locations of one or more receivers. In this section, we abstract away from implementation issues (such as taking over an established lock to legitimate satellites, see Section 5) and assume that there are no legitimate signals present on the channel. The intuition underlying the results that we will present is the following: spoofing requires the attacker to send out signals precisely aligned in time. This will be harder—if not impossible—for increasing numbers of victims (as summarized in Table 2 and visualized in Figure 5).

4.1 Construction of Pseudoranges

The attacker’s physical location $P_i^A$, his transmission time offset $\delta_i^A$, and the claimed satellite position $L_i^A$ all influence the location $L_i^A$ computed by a victim $V_i$ (see Sections 2 and 3.2). By setting his physical location $P_i^A$ and transmission offset $\delta_i^A$, the

Figure 3: Models of the attacker’s antenna coverage. (a) The attacker’s signals reach all victims (used in the analysis of this paper). (b) The attacker’s antennas each only reach one victim. This requires the attacker to be in close proximity to the victims if the distances between the receivers are small.
attacker can influence the pseudorange computation at the victim. The expected pseudorange that a victim at physical position \( P_i \) will compute based on the attacker’s signal \( s^A_i \) is

\[
R^A_{ij} = |P_j - P_i| + \delta^A_{ij} \cdot c
\]  

(6)

To determine its location, each victim solves a system of equations with the calculated pseudoranges (see Figure 4):

\[
|L'_j - L^A_i| = R^A_{ij} - \Delta^A_j
\]  

(7)

Here, \( L^A_i \) are the (claimed) satellite coordinates of \( S_i \) extracted by \( V_j \) from the GPS message, \( R^A_{ij} \) is the pseudorange to satellite \( S_i \) as calculated by \( V_j \) based on the received signal, and \( \Delta^A_j \) is the time offset times propagation speed as calculated by the victim.

For each impersonated satellite, the attacker must send a signal \( s^A_i \) such that solving Equation 7 by the victim yields the target location \( L'_j \) and the target time offset \( \delta'_j \). This requires \( R^A_{ij} = R^A_{ij}' \), or:

\[
|P_j - P^A_i| + \Delta^A_i = |L'_j - L^A_i| + \Delta^A_j.
\]  

(8)

In attacks on civilian GPS, the attacker is free to choose \( P^A_i \), \( \delta^A_i \), and \( L^A_i \). This means that the system of equations (8) is underdetermined for a single victim. The attacker can fix two of the variables to his liking and solve for the third.

When the attack targets a military GPS receiver, the attacker cannot change the data content of the messages and is restricted to \( \delta^A_i \), which is greater than or equal to the transmission delay from the satellite to the attacker. Hence, the claimed satellite location in the message is the correct location of the legitimate satellite: \( L^A_i = L^S_i \). In addition, the attacker is restricted by \( \Delta^A_i \geq |P^A_i - L^S_i| \). We can therefore rewrite Equation 8 as

\[
|P_j - P^A_i| + |P^A_i - L^S_i| \leq |L'_j - L^A_i| + \Delta^A_j
\]  

(9)

Or, using the triangle inequality

\[
|P_j - L^S_i| \leq |L'_j - L^A_i| + \Delta^A_j
\]  

(10)

In the following, let \( b^j_{ijk} \) be the difference in pseudoranges to \( P^A_i \) between \( V_j \) and \( V_k \) (see Equation 6):

\[
b^j_{ijk} = R^A_{ij} - R^A_{ik} = |P_j - P^A_i| - |P_k - P^A_i|.
\]  

(11)

Equally, we define \( b^j_{i'k'} \) as the difference of pseudoranges of the claimed satellite location \( L^A_i \) and the spoofed victim locations \( L'_j \) and \( L'_k \) (see Figure 4):

\[
b^j_{i'k'} = R^A_{i'j} - R^A_{k'} = |L'_j - L^A_i| - |L'_k - L^A_i| + \Delta^A_j - \Delta^A_k.
\]  

(12)

4.2 Spoofing to One Location

**Result 1.** One or more receivers \( V_j \in \mathcal{V} \) can be spoofed to any one location \( L' \) using a single attacker antenna. Spoofing multiple receivers to the same location \( L' \) will generally lead to different time offsets \( \delta'_j \) at each victim.

The reason for this is that the time-differences of arrival of the individual satellite signals determine the location that each receiver will compute. If the spoofed signals are all sent from the same attacker antenna, all victims will obtain the same time-differences. A detailed proof is given in Appendix A, along with a discussion of the resulting time differences at the victims.

4.3 Spoofing to Multiple Locations

We next consider multiple receivers at distinct physical locations \( P_1, \ldots, P_n \), that the attacker tries to spoof to the locations \( L'_1, \ldots, L'_n \). Following Result 1, an attacker can spoof any number of receivers in the transmission range to the same coordinates \( L' \) with differing \( \delta'_j \). If the victims have a way of establishing (coarse) relative distances, e.g., by estimating their respective distances visually, or can detect their mutual time offsets, they are able to detect such attacks. Therefore, we will now focus on attacks in which multiple victims are shifted to a set of new locations that preserve their mutual distances and mutual time offsets.

As stated in Result 1, if the attacker is using only one transmission antenna, any possible placement of this antenna will lead to two victims computing their location to the same coordinates \( L' \), with a small time synchronization error. Hence, the attacker cannot use only one antenna to shift the victims to different locations. We will now show that, using multiple antennas, the attacker can spoof two victims to any locations while preserving their mutual time offsets, with certain restrictions on the time offset in the case of military GPS receivers.

**Result 2.** Two receivers at the physical locations \( P_1 \neq P_2 \) can be spoofed to the locations \( L'_1 \neq L'_2 \) and time offsets \( \delta'_1, \delta'_2 \) if the attacker is free to choose any \( P^A_1 \) and \( L^A_1 \). For each \( s^A \), the possible transmission locations \( P^A_1 \) lie on one half of a two-sheeted hyperboloid defined by \( L^A_1, L^A_2, \delta^A_1, \delta^A_2, \) and \( P_1, P_2 \).

In order to spoof \( V_1, V_2 \) to \( L'_1, L'_2 \) and \( \Delta^A_1, \Delta^A_2 \), the attacker must send each \( s^A \) such that it arrives with the correct delay at the physical locations of the victims, i.e., \( b^j_{i'k'} = \delta^A_j \forall s^A \). As \( b^j_{i'k'} \) is defined by \( L^A_i \), the attacker can always find combinations of \( P^A_i \) and \( L^A_i \) that yield the correct pseudorange (for attacks on civilian GPS). He can then use Equation 8 to find the appropriate \( \delta^A_i \).

In the case of military GPS, the attacker cannot change the claimed placements of the satellites: \( L^A_i = L^S_i \). Hence, \( b^j_{i'k'} \) is determined by the selection of \( L^A_1, L^A_2, \delta^A_1, \delta^A_2 \). In this case, Equation 8 yields one hyperboloid for each \( s^A \) with possible values of \( P^A_i \) and \( \delta^A_i \).

We demonstrate this by giving a simple example: the victims are located at \( P_1 = (1, 0, 0) \) and \( P_2 = (-1, 0, 0) \), the physical distance between the victims is \( |P_1 - P_2| = 2 \). The attacker wants to spoof the two victims to the locations \( L'_1 = (0, 0, 0) \) and \( L'_2 = (0, 2, 0) \), both with time offset zero: \( \Delta^A_1 = \Delta^A_2 = 0 \). The attacker now (arbitrarily) chooses \( L^A_1 = (-3, -2, 0), L^A_2 = (-2, 0, 0) \),
Figure 5: Visualization of possible attacker placements. For (a) two victims, all points on the hyperboloid are viable solutions; for (b) three victims the solutions lie on a curve (red/white intersection); and (c) for four victims only two points are viable solutions (white dots).

and $L_i^A = (-2, 2, 0)$ for the claimed satellite positions in the GPS messages. This determines three hyperboloids relative to $P_1$ and $P_2$ based on $b_{112}', b_{212}'$, and $b_{312}'$.

**Result 3.** A necessary condition for a successful GPS group spoofing attack is that $\forall V_j, V_k, \forall s_l, b_{ijk}' \leq |P_j - P_k|$.

In other words, the difference $b_{ijk}'$ of the perceived pseudoranges of each signal $s_l'$ at any two spoofed victim locations $L_j'$ and $L_k'$ must be smaller than or equal to the distance between the victims’ physical locations $P_j$ and $P_k$. From Equation 11 and the triangle inequality it follows that $b_{ijk}' \leq |P_j - P_k|$. Since it must hold that $b_{ijk}' = b_{ijk}$, if $b_{ijk} > |P_j - P_k|$ for any $s_l$, then there is no possible solution for the attacker’s placement $P_i^A$. Thus we get

$$|P_j - P_k| \geq |L_j' - L_i^A| - |L_k' - L_i^A| + \Delta_j' - \Delta_k'$$

(13)

as a necessary condition for a successful attack.

As we know from Result 2, for two victims, all possible antenna placements for the attacker lie on a hyperboloid defined by $P_1$, $L_j'$, $\delta_j'$ and $L_k'$. We will now extend this result to the case of three and more victims. In the following, we assume that $b_{ijk}' \leq |P_j - P_k|$ is fulfilled $\forall V_j, V_k$ and $\forall s_l$, i.e., it is physically possible to spoof the locations of the receivers.

**Result 4.** In a GPS group spoofing attack on three victims $V_1, V_2, V_3$ to specific locations $L_j'$ and time offsets $\delta_j'$, all possible attacker placements $P_i^A$ lie on the intersection of two hyperboloids defined by $b_{112}', b_{113}'$.

This can be shown by constructing two hyperboloids using $b_{112}'$ and $b_{113}'$ as in Result 2. Both hyperboloids yield the possible placements of attacker’s antennas to achieve the correct pseudorange for $V_1, V_2$ or $V_3, V_1$, respectively. Each point on the intersection of the two hyperboloids has a specific $\delta_i'$ and is at the correct distance to all three victims. Therefore, all points of this space curve are valid $P_i^A$ to solve the group spoofing problem.

We can extend our example from Result 2 by a third victim placed at $P_3 = (1, 5, 0)$, which is spoofed to $L_3' = (1, 1, 0)$ with $\delta_3' = 0$. This reduces the possible locations from the hyperboloid as shown in Figure 5(a) to the intersection curve of the hyperboloids constructed using $b_{112}'$ and $b_{113}'$, as shown in Figure 5(b).

**Result 5.** In a GPS group spoofing attack on four victims $V_1, \ldots, V_4$ to specific locations $L_j'$ and time offsets $\delta_j'$, there are at most two possible placements for $P_i^A$ to impersonate a satellite at $L_i^A$. These are the intersection points of three hyperboloids defined by $b_{112}', b_{113}', b_{114}'$.

As previously, to show this, we consider each signal $s_l'$ separately. By computing $b_{112}', b_{113}', b_{114}'$ (and $b_{111}' = 0$) according to Equation 11 and setting $b_{ijk}' = b_{ijk}$, we can construct three hyperboloids. Their intersection points are possible placements for the antennas of the attacker. As the intersection of two hyperboloids yields a spaced curve, the intersection of three hyperboloids is an intersection of this curve with a third hyperboloid, which results in at most two points. We can also arrive at this number of solutions by considering the system of four quadratic equations based on Equation 7. These can be transformed into three linear and one quadratic equation [1], defining the solutions for the location $L_i^A$ and time offset $\delta_i'$. As the quadratic equation has at most two solutions [1], and each of the linear equations has one unique solution, there are at most two solutions for the attacker’s position and transmission time.

This result can also be observed in our example by adding a fourth victim placed at $P_4 = (10, 0, 0)$, which is spoofed to $L_4' = (-1, 0, 0)$ with $\delta_4' = 0$. The possible placements for the attacker’s antenna is now the intersection of the previously obtained curve with another hyperboloid, yielding two points only (Figure 5(c)).

**Result 6.** In a GPS group spoofing attack on five or more victims $V_1, \ldots, V_n$ to specific locations $L_j'$ and time offsets $\delta_j'$, there is at most one possible placement for $P_i^A$ to impersonate a satellite at $L_i^A$. This is the intersection point of $n - 1$ hyperboloids defined by $b_{112}', \ldots, b_{11n}'$.

This result directly continues our previous reasoning: Each added victim adds another hyperboloid to the set of hyperboloids which must intersect to yield a possible $P_i^A$. For five or more receivers, the set of $(n - 1)$ linear equations and one quadratic equation is overdetermined, and therefore has at most one solution.

From Result 5, we know that for military GPS receivers, there are at most two solutions for a given combination of $P_j, L_j', \delta_j'$, and $L_i^A = L_i^S$. For attacks on civilian GPS receivers, the attacker can influence the position of the two solutions of the system of equations by changing the claimed satellite location $L_i^A$. We will now
Tare represented as augmented row vectors, we can therefore write

\[ s \text{ serves the Euclidean distance).} \]

Each transmitted signal per pair of victims).

\[ \text{(i.e., there is only one specific hyperboloid of attacker positions for} \]

\[ \text{in terms of his antenna placement. For civilian GPS, the attacker} \]

\[ \text{will yield a possible antenna placement} \]

\[ \text{of victims and on the target locations: spoofing all receivers to one} \]

\[ \text{formation}\]

\[ \text{such that the} \]

\[ \text{receiver is now to move the victim to a new location} \]

\[ \text{we say that the receiver} \]

\[ \text{lock takeover attacks using a Spirent GSS7700} \]

\[ \text{GPS signals are sent over a cable to eliminate the influence of the trans-} \]

\[ \text{data sent by the attacker, all discussed imperfections should apply} \]

\[ \text{we assume that the condition of Result 3 holds.} \]

\[ \text{The results in Table 2 show that there are no restrictions on} \]

\[ \text{to half of a two-sheeted hyperboloid. In the table we} \]

\[ \text{affine transformation of the claimed} \]

\[ \text{Summary of results: Table 2 gives an overview of sets of possible} \]

\[ \text{affine transformation to} \]

\[ \text{As a consequence of Results 6 and 7, spoofing five or more receivers} \]

\[ \text{attacker's position for} \]

\[ \text{Spoofing to} \]

\[ \text{Spoofing to multiple} \]

\[ \begin{array}{ccc}
 n & \text{Civ. & Mil. GPS} & \text{Civilian GPS} & \text{Military GPS} \\
 1 & P^A_1 \in \mathbb{R}^3 & - & - \\
 2 & P^A_1 \in \mathbb{R}^3 & \text{set of hyperboloids} & \text{one hyperboloid} \\
 3 & P^A_1 \in \mathbb{R}^3 & \text{set of intersections} & \text{intersection of} \\
 & & \text{of two hyperboloids} & \text{two hyperboloids} \\
 4 & P^A_1 \in \mathbb{R}^3 & \text{set of 2 points} & 2 \text{ points} \\
 \geq 5 & P^A_1 \in \mathbb{R}^3 & \text{set of points} & 1 \text{ point} \\
\end{array} \]

\[ \text{Table 2: Summary of results for the number of possible attacker locations} P^A_i \text{ for} \]

\[ n \text{ victims.} \]

\[ \text{give an intuition where these solutions are located for a formation-} \]

\[ \text{preserving GPS spoofing attack.} \]

\[ \text{Result 7. When spoofing a group of GPS receivers} V_i, \ldots, V_n \text{ such that the formation (i.e., the mutual distances} \]

\[ \text{with respect to random noise or environmental changes, the attacker ideally} \]

\[ \text{we say that the receiver} \]

\[ \text{lock on a specific transmitter when it is already receiving data} \]

\[ \text{Since a spoofing signal is likely to be misaligned (in phase, Doppler} \]

\[ \text{we conduct experiments to evaluate the influence of such imperfections.} \]

\[ \text{as we do not change the claimed location of the satellite in the data} \]

\[ \text{GPS receiver in our experiments is an Antaris evaluation kit by u-} \]

\[ \text{in Section 3 we assumed a strong attacker, who is always able to} \]

\[ \text{generate signals with} \]

\[ \text{perfect knowledge of his own and the victim’s position. In a practi-} \]

\[ \text{attacks, many of these assumptions might be invalid. We conduct} \]

\[ \text{all imperfects are discussed uniformly applicable to} \]

\[ \text{we conduct experiments to evaluate the influence of such imperfections.} \]

\[ \text{The results in Table 2 show that there are no restrictions on the} \]

\[ \text{with the victim losing the ability to calculate its position, even for a} \]

\[ \text{we say that the receiver} \]

\[ \text{lock takeover attacks using a Spirent GSS7700} \]

\[ \text{The GPS signal simulator is a hardware device that generates GPS signals} \]

\[ \text{In Section 3 we assumed a strong attacker, who is always able to} \]

\[ \text{generate signals with} \]

\[ \text{we conduct experiments to evaluate the influence of such imperfections.} \]

\[ \text{As we do not change the claimed location of the satellite in the data} \]

\[ \text{we conduct experiments to evaluate the influence of such imperfections.} \]

\[ \text{The results in Table 2 show that} \]

\[ \text{with the victim losing the ability to calculate its position, even for a} \]

\[ \text{we conduct experiments to evaluate the influence of such imperfections.} \]

\[ \text{As we do not change the claimed location of the satellite in the data} \]

\[ \text{we conduct experiments to evaluate the influence of such imperfections.} \]

\[ \text{The results in Table 2 show that there are no restrictions on the} \]

\[ \text{We conduct the lock takeover attacks using a Spirent GSS7700} \]

\[ \text{The GPS receiver in our experiments is an Antaris evaluation kit by} \]

\[ \text{at the start of each experiment, we send only the legitimate GPS} \]

\[ \text{signals are sent over a cable to eliminate the influence of the trans-} \]

\[ \text{This enables us to measure the unique influence of the parameters of} \]

\[ \text{we conduct the lock takeover attacks using a Spirent GSS7700} \]

\[ \text{The GPS receiver in our experiments is an Antaris evaluation kit by u-} \]

\[ \text{At the start of each experiment, we send only the legitimate GPS} \]

\[ \text{We conduct the lock takeover attacks using a Spirent GSS7700} \]

\[ \text{The GPS receiver in our experiments is an Antaris evaluation kit by} \]

\[ \text{At the start of each experiment, we send only the legitimate GPS} \]

\[ \text{We conduct the lock takeover attacks using a Spirent GSS7700} \]

\[ \text{The GPS receiver in our experiments is an Antaris evaluation kit by u-} \]

\[ \text{At the start of each experiment, we send only the legitimate GPS} \]

\[ \text{We conduct the lock takeover attacks using a Spirent GSS7700} \]

\[ \text{The GPS receiver in our experiments is an Antaris evaluation kit by} \]

\[ \text{At the start of each experiment, we send only the legitimate GPS} \]
The attack then consists of two phases: first, the attacker sends signals which are supposed to match the legitimate satellites’ signals at the location of the victim. These are generated by the attacker by approximating the current location of the victim as \( L_{\text{init}} \), and constructing signals with time delays and data content appropriate for that location (see Section 4.1). This first phase lasts for one minute to allow the victim to lock on to the new signals. In the second phase, the attacker start to move the spoofed location towards the final location \( L' \), imitating an acceleration of 0.5m/s\(^2\). After 3 minutes, the final location is reached. If this final location is not remotely close to \( L' \) (height difference \( \leq 150 \text{m} \), horizontal distance \( \leq 1 \text{km} \)), we consider the takeover failed.

We vary the distance between the victim’s true location \( L \) and its initial location as assumed by the attacker \( L_{\text{init}} \) as one of the parameters in the experiments. We refer to this distance as the location offset \( d_{\text{init}} = |L - L_{\text{init}}| \). The other parameters we investigate are relative signal power, relative time offset and constant time offset. For each parameter value, five experiments were run.

We say that the lock takeover was successful if at the end of the experiment the victim’s final location is close to \( L' \). If the victim is close to \( L' \) but was unable to compute a valid position for more than one second during the lock takeover, we consider the attack a partial success and use the number of seconds the victim was not able to calculate a valid position as an error metric.

5.2 Results of the Experiments

Relative signal power of the spoofing signal: In this experiment, ideal spoofing signals are sent, but the power of the spoofing signals is varied between \(-2 \text{dB}\) and \(+8 \text{dB}\) relative to the legitimate signals. Figure 7(a) shows the effect of using spoofing signals that have the same power as the legitimate signals. In this figure, \( t_s \) marks the time when the spoofing location starts to move away from \( L_{\text{init}} \). The errors in longitude, latitude, and height are shown separately and are measured between the location as reported by the receiver and the one sent by the simulator. Although the victim reports the spoofed location for some time, it switches back to \( L \) after 170s of the experiment, which causes the growing error in longitude.

Figure 7(b) shows the error in meters between the position reported by the GPS receiver and the location sent by the attacker, as a function of the relative power of the attacker’s signals. The error bars show the standard deviation for the error value over the five experimental runs. The gray bars indicate the ratio of attempts in which the victim lost lock completely during the takeover. To evaluate the smoothness of the lock takeover, if the receiver reported a location too far away from \( L' \), we count this run as failed takeover. Blue bars in the figure denote the ratio of attempts in which the GPS receiver was unable to compute a valid location.

It can be seen that for at least 2dB more power, the receiver consistently locks on to the spoofing signals without any offset occurring. 2dB of power is sufficiently low to not be detected by power based spoofing-countermeasures in practice.

Constant time offset influence: The second question we investigate is the effect of a general delay on all signals sent by the attacker relative to the legitimate signals. Such time delays can occur if the attacker’s system setup is not perfectly compensating for internal delays, the distance to the victim is unknown or the system clock of the attacker is not synchronized perfectly to the clock of the legitimate GPS satellites. The interesting question is if such a general time offset will result in detectable errors in the victim’s reported position, and if such a time offset will increase the chance of the victim losing lock completely during the takeover. To evaluate the influence of a constant time offset, we run the tests with time off-
Location offset influence: In this series of experiments we determine the influence of an offset $d_{\text{init}}$ between the position of the victim as determined from the legitimate satellites $L$ and the spoofing signals sent by the attacker $L_{\text{init}}$. We evaluate the influence of such a location offset for values between 0 and 450m. Similarly to the time offset, this location offset can lead to a relatively large error during the lock takeover. An example with offset of 340m is given in Figure 8(a).

In Figure 8(b), we show the average error as a function of the location offset. Regardless of the intermediate errors, eventually the victim always synchronizes to the attacker’s signals in all our experiments. This shows that the initial position is not very sensitive to small errors. If an attacker knows the location of his victim to within about 100 meters, he can perform a smooth takeover without the victim losing lock. A value of 340m roughly corresponds to a distance of 22.5m, meaning that the attacker must know his distance from the victim with an accuracy of 22.5m (or better) — a higher offset will cause the victim to lose lock due to the signal (chip phase) misalignment. We confirmed that the initial location offset will cause

by inaccuracies in the delay setup in the case of military GPS signals. In this experiment, we evaluate the consequences of having half of the spoofed satellite signals shifted by a fixed amount of time relative to the other half of the signals. In Figure 8(c), we show an example run with a time delay mismatch of 140ns. (d) Average error over the time delay mismatch as a function of the time delay mismatch.

Relative time offset influence: In the case where the attacker has access to more than one transmission antenna, he can send the spoofing signals using two or more omnidirectional antennas (see Section 4). Depending on the relative position of the individual antennas, the victim will receive the spoofing signals with different time delays. Relative time offsets of the signals can also be caused

sets between 0ns and 240ns. We plot the location error between the attacker’s intended location and the actual location reported by the victim an example run in Figure 7(c). The effects are consistent over several runs with the same parameters, but can vary quite a lot with these parameters.

In Figure 7(d), we show the general relation between the average errors during the measurement as a function of the time offset for the first 120ns. After this time, lock takeover was not working consistently any more.

We conducted the above experiments in order to evaluate the effects of imperfections in the attacker’s signals for lock-takeovers. As these effects are influenced by the actual hardware at the receivers, the exact values might differ for other types of receivers, but the fundamental relations will remain the same. The results are summarized in Table 3.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative signal power</td>
<td>$\geq +2\text{dB}$</td>
</tr>
<tr>
<td>Constant time offset</td>
<td>$\leq 75\text{ns}$</td>
</tr>
<tr>
<td>Location offset</td>
<td>$\leq 500\text{m}$</td>
</tr>
<tr>
<td>Relative time offset</td>
<td>$\leq 80\text{ns}$</td>
</tr>
</tbody>
</table>

Table 3: Required parameter ranges for seamless lock-takeover in a GPS spoofing attack in our experiments.
a noticeable jump of the victim's reported position during the attack. Large offsets could therefore be detected by the victim by monitoring its position. Any imperfections in the arrival time of the signal from different antennas will directly impact the position calculated by the victim. If the relative offset gets above 80ns, the signals will even cause the receiver to lose lock. This means that, if an attacker has multiple antennas, he must precisely know the distance from each antenna to the attacker in order to be able to spoof a desired location. We could also observe a general localization error as predicted in our theoretical analysis, even for smaller mismatches in the arrival times.

6. GPS SPOOFING COUNTERMEASURE

Spoofing detection based on lock loss has two disadvantages: (i) strong attackers can achieve a seamless satellite-lock takeover, and (ii) lock loss can occur due to natural causes (e.g. signal loss in a tunnel). We propose a countermeasure against GPS spoofing attacks that does not rely on the signal analysis or on the lock loss of signal. Instead, our mechanism is based on our insights of Section 4 and relies on the use of several GPS receivers. These GPS receivers can be deployed in a static, known formation, e.g., they are fixed on the deck of a cargo ship (see Figure 9). The basic idea of the countermeasure is the following: If the GPS receivers can exchange their individual GPS locations, they can check if their calculated locations preserve their physical formation (within certain error bounds). In the case that the calculated GPS locations do not match the known formation, an attack must be suspected and there should be a warning message.

Even if only two GPS receivers are used, this countermeasure can detect any attacker that is only using a single antenna. As shown in Result 1, in case of a single-antenna attack both GPS receivers would report the same location (with small time offsets).

As shown in Results 4-6, a strong attacker using multiple antennas could attempt to send signals such that the mutual distances between multiple receivers are preserved. Nevertheless, each additional receiver of the victim makes these spoofing attacks exceedingly more difficult because the space of possible antenna placements for the attacker gets reduced significantly (see Table 2). From Results 6 and 7 we know that there exists only one location per satellite where the attacker can place his antenna; this location is the rotated and translated satellite position of the GPS signal. Conducting such an attack is very difficult. It becomes even impossible if the victim can hide the exact positioning of at least one GPS receiver from the attacker (e.g., by keeping it mobile on the vehicle) such that the attacker cannot adapt to its position.

In summary, our countermeasure requires no modifications of the GPS signal, the satellite infrastructure, or the GPS receiver, it is resistant against a wide range of attackers, and it can be deployed using multiple standard GPS receivers.

Outlook: Further possible applications are not restricted to mobile scenarios with a fixed formation (such as in the cargo ship example above). The countermeasure can also be applied (i) to fixed and static (i.e., immobile) settings where GPS is used for time synchronization and (ii) to mobile settings with varying formations (e.g., mobile formation of cars, robots, etc.). In the latter case, the devices can apply additional ranging techniques to identify their formation and use it in the sanity check with the calculated GPS locations (as long as the ranging techniques are secure [2,6,10,18,21]). We leave the elaboration of these ideas for future work.

7. CONCLUSION

In this paper, we analyzed the requirements for successful GPS spoofing attacks on individuals and groups of victims with civilian or military GPS receivers. In particular, we identified from which locations and with which precision the attacker needs to generate its signals in order to successfully spoof the receivers.

For example, we show how spoofing a group of victims can only be achieved from a restricted set of locations, if the attacker aims to preserve the mutual distances and time offsets of the victims. With growing size of the group of victims, less spoofing location become available, until only single points remain for 5 victims or more. In addition, we discussed the practical aspects of seamless satellite-lock takeover. We used a GPS signal generator to perform a set of experiments in which we investigated the required precision of the attacker’s spoofing signals. Besides demonstrating the effects of such lock takovers on the victim, our results include minimal bounds for critical parameters to allow a seamless takeover of our target platform. Finally, we proposed a technique for the detection of spoofing based on a group of standard GPS receivers (without specific spoofing detection measures) in a static formation.

Acknowledgments

This work was partially supported by the Zurich Information Security Center. It represents the views of the authors.

8. REFERENCES

To show Result 1, we first focus on a single receiver $V_1$ and civil-
ian GPS. The attacker selects a target location $L'$, a target time
offset $\delta'_1$, and any arbitrary attacker location $P_1^A$. Given this, Equation 8 yields $\Delta'_1$. Using one transmission antenna (i.e. $P_1^A = P_2^A \forall j \neq 3$), the attacker transmits all signals $s_1^A$ with the delay $\delta'_1/c$.

While this will successfully spoof the location and time of one
victim, other victims in the vicinity will receive the same signals with slight time delay or advancement. We now consider a set of receivers $V = \{V_1, \ldots, V_n\}$ that are positioned at different physical
locations $P = \{P_1, \ldots, P_n\}$.

Since the attacker sends all signals $s_1^A$ from the same position $P_1^A = P_2^A = \ldots$, we can follow that $b_{1jk} = b_{2jk} = \ldots$ for all signals $s_1^A$. To compute the effect of the offset on the pseudoranges on each victim, we can express each victims’ pseudorange relative to the pseudorange of the first victim: $R_{ij} = R_{i1} + b_{ijk}$. Each victim will measure pseudoranges based on their physical distances to the attacker: $R'_{ij} = R_{i1}'$. We can now substitute (11) into (7) and get the following equation for each signal $s_1^A$ and $V_j$:

$$|L'_1 - L_i^A| = R'_{i1} - (\Delta'_1 - b_{13j}).$$

Thus, for every $V_j$, these equations only differ by the different value $(\Delta'_1 - b_{13j}) = \Delta'_j$. This means that all $V_j$ compute an identical location $L'$, but different clock offsets $\delta'_j$:

$$\delta'_j = \delta'_1 + \frac{1}{c}(|P_j - P_{1}^A| - |P_1 - P_{1}^A|).$$

Result 1 shows that an attacker can make a group of victims believe to be at a specific location by sending one set of satellite signals from the same antenna. All victims will believe to be at the same location $L'$, but with different time offsets. The additional time offset $\delta'_j - \delta'_1$ between victim $V_j$ and $V_k$ introduced by the attacker is bounded by their mutual distance $|\delta'_j - \delta'_1| \leq |L'_1 - L'_2|$ and is typically on the order of nanoseconds for victims a few meters apart.

In attacks on military GPS, Equation 10 can be used to derive the additional constraints on the relation between the resulting time offset of the main victim $\delta'_1$ and the distance between the spoofed location and each satellite.

\[\text{APPENDIX}\]

A. PROOF OF RESULT 1

For the victim to be able to compute its location, it must hold that the claimed locations are mutually different $L_1^A \neq L_2^A \neq \ldots$. 


[7] Humphreys, T. E., Ledvina, B. M., Pissiak, M. L.,
O’Hanlon, B. W., and Kintner, P. M. Assessing the
spoofing threat: Development of a portable GPS civilian
spoof system. In Proceedings of the ION GNSS International

[8] John A. Volpe National Transportation Systems
Center. Vulnerability assessment of the transportation
infrastructure relying on the global positioning system. Final

tracking = high security? Think again. In Proceedings of

UWB impulse radio based distance bounding. In
Proceedings of the Workshop on Positioning, Navigation and
Communication (WPNC) (2010).

navigation signals. In Proceedings of the Information Hiding

[12] Ledvina, B. M., Bencze, W. J., Galusha, B., and
Miller, I. An in-line anti-spoofing device for legacy civil
GPS receivers. In Proceedings of the ION International
Technical Meeting (2010).

B. M. Receiver-autonomous spoofing detection:
Experimental results of a multi-antenna receiver defense
against a portable civil GPS spoofer. In Proceedings of the

[14] Motella, B., Pini, M., Fantino, M., Mulassano, P.,
Nicola, M., Fortuny-Guasch, J., Wildemeersch,
M., and Symeonidis, D. Performance assessment of low
cost GPS receivers under civilian spoofing attacks. In
Proceedings of ESA Workshop on Satellite Navigation
Technologies and European Workshop on GNSS Signals and


[16] Papadimitratos, P., and Jovanovic, A. GNSS-based
Positioning: Attacks and countermeasures. In Proceedings of
the IEEE Military Communications Conference (MILCOM)
(2008).

[17] Papadimitratos, P., and Jovanovic, A. Protection and
fundamental vulnerability of GNSS. In Proceedings of the
International Workshop on Satellite and Space
Communications (2008).

[18] Rasmussen, K. B., and Capkun, S. Realization of RF
distance bounding. In Proceedings of the USENIX Security
Symposium (2010).

[19] Scott, L. Anti-spoofing & authenticated signal
architectures for civil navigation systems. In Proceedings of
the ION GNSS International Technical Meeting of the
Satellite Division (2003).

[20] Spirent Communications plc. SimGEN simulation

[21] Tippenhauer, N. O., Rasmussen, K. B., and Čapkun,
S. Secure ranging with message temporal integrity. In

system. standard positioning service. performance standard,
Sep 2008.


demonstration that the global positioning system (GPS) is
vulnerable to spoofing. Journal of Security Administration
(2002).