Impacts of a Single GPS Spoofer on Multiple Receivers: Formal Analysis and Experimental Evaluation

Wenxin Chen, Yingfei Dong
Department of Electrical Engineering
University of Hawaii
Honolulu, HI 96822

Zhenhai Duan
Department of Computer Science
Florida State University
Tallahassee, FL 32306

***Abstract*—As many mobile devices use Global Navigation Satellite Systems (GNSSs) to determine their locations for control, compromising such systems can result in serious consequences, as shown by existing GPS spoofing attacks. However, most such spoofing attacks focus on the effect of a single spoofer attacking a single receiver. In this paper, we investigate the impacts of a single spoofer on multiple receivers, motivated by research on attacking drone swarms. Our analysis independently shows that, using a single spoofer, multiple receivers at different locations in a spoofing area will see the same location reading. We consider the base case of spoofing four satellites and also the generic case when more satellites are involved in the spoofing attack. More importantly, we conduct real-world experiments to validate our analysis and demonstrate the potential threats to many practical applications. We use off-the-shelf SDR cards for spoofing and consumer GPS receivers for obtaining spoofed location readings. While this method can enable various attacks on mobile devices depending on GPS, it is also applicable to all existing GNSSs, because they use similar principles to determine locations.**

***Index Terms*—GNSS, GPS Spoofing, Drone Countermeasures**

I. Introduction

Since the Global Positioning System (GPS) system was open for civil use in 2000, it has been adopted by many civil applications, such as air transportation, naval navigation, and geographical land survey. Following the success of GPS, other GNSSs have also been developed such as Galileo, GLONASS, etc. In the past two decades, the cost of a GPS receiver has been dramatically reduced such that it becomes a common device on many mobile devices to support routine operations, e.g., a consumer drone performs auto-piloted missions based on GPS. However, because the civil GPS signal is fairly weak and is not protected with a proper authentication method, GPS spoofing attacks have been explored in many projects [1], [2], [3], [4]. To the best of our knowledge, existing methods mostly focused on the effect of a single spoofer on a single receiver, except the limited analysis of spoofing multiple receivers in [5]. Therefore, we focus on the impacts of a single spoofer on multiple receivers in this paper.

This work was motivated by the exploration of attacking a drone swarm via GPS spoofing. As an auto-piloted drone swarm usually performs its mission based on GPS, compromising the GPS readings of these drones is an interesting method to deal with the swarm. As the first step in this direction, we need to figure out the concrete impacts that a single spoofer may have on a drone swarm. There have been a number of projects using GPS spoofing to attack individual drones [6], [7], [8]. However, none of them systematically analyzed the impacts of GPS spoofing on multiple drones.

Our analysis in this paper shows an interesting result: when spoofed GPS signals overpower the authentic signals such that GPS receivers in the spoofing area are all locked to the spoofed signals, these receivers at different locations will see the same location reading. Due to the inherent properties of location determination algorithms on GPS receivers, the algorithms will give the same solution as we show in this paper, although they are at different physical locations in the spoofing area. We further conduct real-world experiments to confirm our analysis, and show the potential threats of such attacks. Although the attack discussed in this paper shows the impact at the GPS signal level, more powerful attacks can be developed to further deceive drone state estimation and navigation control algorithms to disrupt their missions.

We use a method similar to existing GPS spoofing attacks: using off-the-shelf *Software Defined Radio* (*SDR*) cards (such as *USRPs*, *BladeRF* cards, *HackRF* cards, and *RTL-SDR* dongles) and open-source GNSS and GPS software (such as *GPS-SDR-SIM*, *BladeGPS*, *GNSS-SDR*, and *gpsd*), we are able to conduct in-depth analysis of concrete steps in GPS signal processing, such as receiving, decoding, and regenerating. Utilizing these tools, we experiment with various GPS receiving, manipulating, and transmission settings. We observe a surprising phenomenon: multiple receivers at different locations within the spoofing area always have very similar location readings. This interesting result motivates us to dive into the details of GPS location determination process, and eventually find out the reason behind this observation. As all GNSSs use similar principles to determine locations, this result clearly reveals a generic threat to all such systems.

The main contribution of this paper is that, via both comprehensive theoretical analysis and real-world experiments, we clearly identify the impacts of a single GPS spoofer on multiple receivers at different locations in the spoofing area. We analyze both the base case of spoofing four satellites and the generic case when more satellites are involved. We further conduct real-world experiments with broadly available SDR cards to validate our analysis, and demonstrate the real threats to a group of GPS receivers.

The remainder of this paper is organized as follows. We

first introduce the basics of GPS, GPS spoofing, and related work in Section 2. We then discuss the system setup and the attack model, and present the analysis of the impacts of a single spoofer on multiple receivers in Section 3. We discuss the experimental evaluation in Section 4. We further conclude this paper and discuss future work in Section 5.

II. Related Work

In this section, we first introduce the GPS basics, and further discuss GPS spoofing methods and several related projects.

A. GPS Basics

Civil GPS is arguably the most popular positioning system for mobile devices, such as consumer drones and many other applications. The GPS system consists of three segments: the satellite segment (satellite constellation), the ground segment (ground control network), and the user segment (user equipment) [9]. There are multiple sets of GPS satellites for different purposes. Here we focus on the set of satellites broadcasting civil signals. It maintains at least 24 satellites available around the globe; we can observe about 6 to 12 satellites at any location on the surface of the globe.

Each satellite orbits in a predefined track and continuously broadcasts a 1500-bit GPS frame every 30 seconds. Each GPS frame has five subframes. Subframe 1 contains the GPS week number, satellite accuracy and health, and satellite clock correction terms; subframes 2 and 3 contain the satellite's precise orbital ephemeris information, giving the predicted positions of the satellite at regular time intervals from 30 minutes up to four hours; subframes 4 and 5 carry 1/25 of almanac information about the predefined tracks of all 32 satellites and is used for predicting which satellites may be observable based on a receiver's (estimated) location. Furthermore, a complete GPS message is delivered in 25 frames. In this paper, we focus the civil GPS signals at 1575.42 MHz with the Coarse/Acquisition (C/A) code on the L1 band. The C/A code is not encrypted for civil access. (The high-resolution military GPS signals are broadcast in an encrypted precision (P/Y) code on the L2 band at 1227.60MHz to authorized receivers, which is not the subject we discuss here.)

For a GPS receiver to determine its location, it needs to be locked on at least four satellites and find the distances (pseudo-ranges) to these satellites. As shown in Figure 1, t is the GPS system time; dT_j is the clock bias between a receiver R_j's local time and the GPS system time t; $t_j^{(i)}$ is the receiving time of a frame from satellite i at receiver R_j. We first consider the base case of four satellites. The pseudo-range $p_j^{(i)}$ from R_j at position $(x_{R_j}, y_{R_j}, z_{R_j})$ to satellite i at position $(x^{(i)}, y^{(i)}, z^{(i)})$ is defined as $p_j^{(i)} = \sqrt{(x^{(i)} - x_{R_j})^2 + (y^{(i)} - y_{R_j})^2 + (z^{(i)} - z_{R_j})^2} + c \cdot dT_j = c \cdot (t_j^{(i)} - t)$, where c is the speed of light. Then the system of equations for a GPS solution in the base case is:

$$\begin{cases} p_j^{(1)} = \sqrt{(x^{(1)} - x_{R_j})^2 + (y^{(1)} - y_{R_j})^2 + (z^{(1)} - z_{R_j})^2} \\ \qquad + c \cdot dT_j, \\ p_j^{(2)} = \sqrt{(x^{(2)} - x_{R_j})^2 + (y^{(2)} - y_{R_j})^2 + (z^{(2)} - z_{R_j})^2} \\ \qquad + c \cdot dT_j, \\ p_j^{(3)} = \sqrt{(x^{(3)} - x_{R_j})^2 + (y^{(3)} - y_{R_j})^2 + (z^{(3)} - z_{R_j})^2} \\ \qquad + c \cdot dT_j, \\ p_j^{(4)} = \sqrt{(x^{(4)} - x_{R_j})^2 + (y^{(4)} - y_{R_j})^2 + (z^{(4)} - z_{R_j})^2} \\ \qquad + c \cdot dT_j \end{cases} \tag{1}$$

At receiver R_j, we have four pseudo-range equations to solve four unknowns (three position coordinates $(x_{R_j}, y_{R_j}, z_{R_j})$ and a clock bias dT_j). There is only one solution to this system of equations. In the general case of more than four satellites available, the system of GPS equations at a receiver would be over-determined. Specifically, assume there are $N > 4$ satellites available for R_j, there will be N equations in the system of eqs. 1. However, there are only four unknowns: x_{R_j}, y_{R_j}, z_{R_j}, and dT_j. Therefore, eqs. 1 is over-determined. Usually, the GPS system uses the common least-squares method to solve this problem. For the $N > 4$ case, we defined the following series of functions for R_j:

$$\begin{aligned} & f^{(i)}(x_{R_j}, y_{R_j}, z_{R_j}, dT_j) \\ =& \sqrt{(x^{(i)} - x_{R_j})^2 + (y^{(i)} - y_{R_j})^2 + (z^{(i)} - z_{R_j})^2} \\ & + c \cdot dT_j - p_j^{(i)}, \end{aligned} \tag{2}$$

for $i = 1, 2, 3, \ldots, N$. Then, the best estimation of the four unknowns: $x_{R_j}^*$, $y_{R_j}^*$, $z_{R_j}^*$, and dT_j^* will be:

$$\underset{x_{R_j}, y_{R_j}, z_{R_j}, dT_j}{\arg\min} \sum_{i=1}^{N} [f^{(i)}(x_{R_j}, y_{R_j}, z_{R_j}, dT_j)]^2. \tag{3}$$

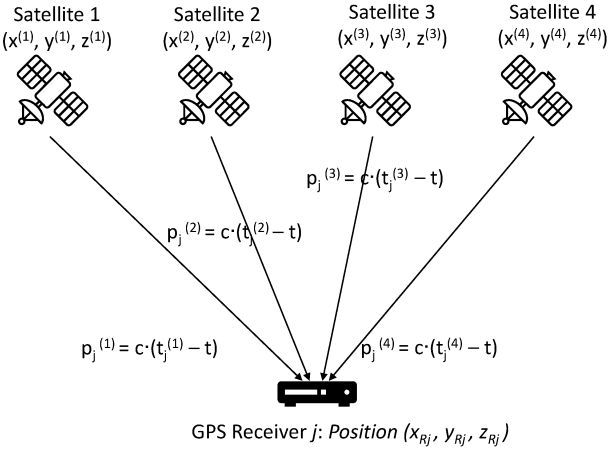

Fig. 1: Flow path of the authentic GPS signal transmission.

B. GPS Spoofing

The vulnerability of civil GPS service was first identified in 2001 [10], and further accessed by the sentinel work in 2008 [1]. Furthermore, various GPS spoofing attacks were proposed by generating GPS signals via simulators or shifting the authentic GPS signals to fool victim receivers [1], [11]. While early experiments used customized special devices to exploit the vulnerability, recent low-cost off-the-shelf SDR devices make GPS spoofing a much broad threat to many systems, especially when more mobile devices are dependent on GPS, such as drones, autopiloted cars, etc. [2], [3], [4].

The main idea of civil GPS spoofing is to trick a GPS receiver into tracking counterfeit GPS signals, instead of the authentic GPS signals. Since the authentic GPS signals are fairly weak and not authenticated, it is easier to produce stronger signals using a local transmitter to overpower the authentic GPS signals, via customized devices [1] or SDR devices [2], [3], [4].

Several projects have shown practical attacks on real-world systems such as drones [6], [7], [8], [12], [13] and route-planning applications [3]. Utilizing SDR devices, such an attack compromises the GPS readings of a target receiver such that its application mission is disrupted. However, most of these attacks focus on a single receiver, and have not systematically considered the issue of multiple receivers, which is the focus of this paper. In [5], the author presented some results about GPS spoofing on multiple receivers. However, our analysis is more generic, because we further investigate beyond the base case of four satellites, and formulate the analysis for the general case of spoofing more than four satellites. Note that during most of our real-world tests, a receiver will see more than four satellites. For some devices (such as a 3DR Solo drone), it will not take off until it sees at least six satellites. The base case only needs to solve four equations for four unknowns; the generic case has more than four equations for four unknowns, which is overdetermined and needs to be solved using an optimization method such as the least-squares. In addition, to validate the analysis, we conducted real-world experiments with SDR cards and GPS receivers, while [5] validated their analysis only in simulated environments.

III. Analysis of Spoofing Impacts on Multiple Receivers

In the following, we will first introduce the system setup and the attack model for the multiple-receiver case, and then present the formal analysis of the impacts of a single spoofer on multiple receivers at different locations in the spoofing area.

A. System Setup and Attack Model

While multiple projects have used GPS spoofing to successfully attack a single drone, there is still no clear method on how to attack a drone swarm using GPS spoofing. This paper focuses on this issue, and investigates the impacts of GPS spoofing on a group of receivers. In the following, we introduce our attack model and an attack framework that utilizes off-the-shelf SDR devices and open-source software to carry out GPS spoofing attacks. We will discuss the generation of spoofing GPS signals based on the latest GPS ephemeris data and intended spoofing locations, and then transmitting them to GPS receivers. In the next subsection, we further analyze the impacts of GPS spoofing on different receivers in this environment.

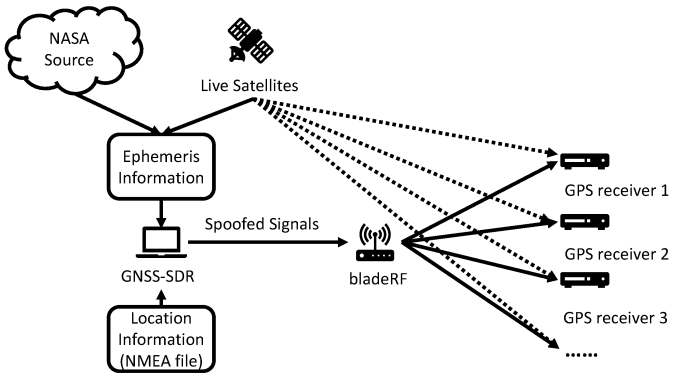

Fig. 2: Attack model of the proposed attack.

Attack Model. As shown in Figure 2, we forge GPS signals based on the satellite ephemeris data and the intended spoofing locations (specified in the National Marine Electronics Association (NMEA) format), and then transmit the spoofed signals via a bladeRF card to GPS receivers. As the spoofing signals (shown as the solid lines) are stronger than the signals from satellites (shown as dashed-lines), the GPS receivers will lock to the spoofing signals.

We build and broadcast the spoofing GPS signals in three steps. First, we obtain the latest ephemeris data. This can be done in two ways: one method is to download satellite ephemeris in the form of a Receiver Independent Exchange Format (RINEX) file from the NASA official site [14], and another method is to obtain live ephemeris from satellites directly. In the experiments, we use the first method because it is simple and sufficient for our tests. Second, we generate the spoofing GPS signal bitstreams using the GPS-SDR-SIM tool. Finally, we broadcast the generated bitstreams using a bladeRF card to GPS receivers in the coverage area.

B. Analyzing Impacts of Single Spoofer on Multiple Receivers

In this paper, we focus on the case of a single spoofer. Using a single spoofer, the paths of the spoofed signal transmission are illustrated in Figure 3, different from the normal paths of authentic signal transmission shown in Figure 1. Here we first consider the base case that a receiver uses four satellites to determine its location. We will then discuss the generic case with more than four satellites later. We assume that the spoofer sends the spoofing signals of all the four satellites. We first create the intended spoofing locations in a NMEA file that specifies the set of intended spoofing locations over a period of time. Then, we build the spoofing signals based on the NMEA file and the latest ephemeris file so that the

TABLE I: Notation Table.

c	Speed of light
R_j	GPS receiver j
$p^{(i)}$	Pseudo range between the Satellite i and the spoofer
$p_j^{(i)}$	"Pseudo range" between the Satellite i and R_j
D_j	Distance between the spoofer and R_j
$(x^{(i)}, y^{(i)}, z^{(i)})$	3D location of Satellite i
$(x_{R_j}, y_{R_j}, z_{R_j})$	3D GPS location solution with regard to R_j
dT_j	Receiver j's clock bias
N	Number of available satellites
$x^*_{R_j}$, $y^*_{R_j}$, $z^*_{R_j}$, and dT^*_j	3D GPS location and clock bias solution with regard to R_j in the case of $N > 4$

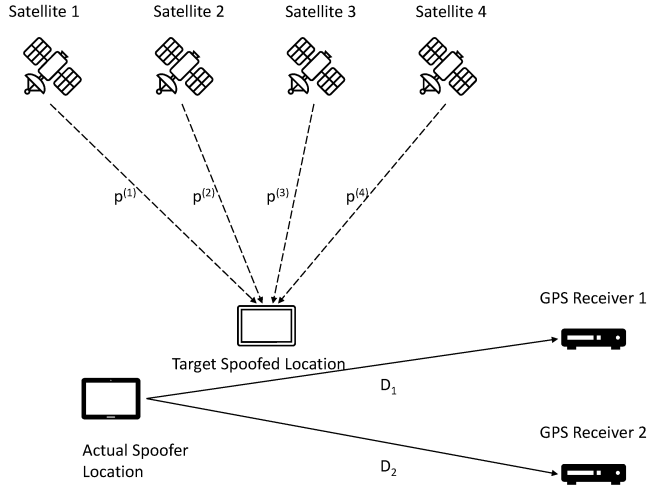

Fig. 3: Flow path of the spoofed GPS signal transmission.

signals can result in the desired localization solution at each given time step.

As we mentioned in Section II-A, each pseudo range $p^{(i)}$ between the Satellite i and the spoofer is obtained based on the following equation:

$$p^{(i)} = c \cdot (t_{sp} - t), \tag{4}$$

where c is the speed of light, t_{sp} is the signal transmitting time at the spoofer, and t is the GPS system time. However, the tricky issue in this case is that there is another transmission step between the spoofer and each GPS receiver. Therefore, for each GPS receiver R_j, the perceived pseudo range $p_j^{(i)}$ between the Satellite i and the GPS receiver will be:

$$p_j^{(i)} = p^{(i)} + c \cdot (t_{R_j} - t_{sp}) = p^{(i)} + D_j, \tag{5}$$

where t_{R_j} is the signal receiving time at R_j, and D_j is the distance between the spoofer and R_j. Here D_j is equal to the sum of the true distance between the spoofer and R_j plus a small error term caused by the offset between their clocks $c \cdot (dT_j - dT_{sp})$, which can be regarded as a constant.

Then according to the GPS algorithms, for the 3D GPS location $(x_{R_1}, y_{R_1}, z_{R_1})$ of Receiver R_1 at local time t_{R_1}, we have:

$$\begin{cases} p_1^{(1)} = \sqrt{(x^{(1)} - x_{R_1})^2 + (y^{(1)} - y_{R_1})^2 + (z^{(1)} - z_{R_1})^2} \\ \qquad + c \cdot dT_1, \\ p_1^{(2)} = \sqrt{(x^{(2)} - x_{R_1})^2 + (y^{(2)} - y_{R_1})^2 + (z^{(2)} - z_{R_1})^2} \\ \qquad + c \cdot dT_1, \\ p_1^{(3)} = \sqrt{(x^{(3)} - x_{R_1})^2 + (y^{(3)} - y_{R_1})^2 + (z^{(3)} - z_{R_1})^2} \\ \qquad + c \cdot dT_1, \\ p_1^{(4)} = \sqrt{(x^{(4)} - x_{R_1})^2 + (y^{(4)} - y_{R_1})^2 + (z^{(4)} - z_{R_1})^2} \\ \qquad + c \cdot dT_1, \end{cases} \tag{6}$$

where $(x^{(i)}, y^{(i)}, z^{(i)})$ is the location of Satellite i, and dT_1 is the receiver clock bias of R_1.

For the 3D GPS position $(x_{R_2}, y_{R_2}, z_{R_2})$ of Receiver R_2 at local time t_{R_2}, we have

$$\begin{cases} p_2^{(1)} = \sqrt{(x^{(1)} - x_{R_2})^2 + (y^{(1)} - y_{R_2})^2 + (z^{(1)} - z_{R_2})^2} \\ \qquad + c \cdot dT_2, \\ p_2^{(2)} = \sqrt{(x^{(2)} - x_{R_2})^2 + (y^{(2)} - y_{R_2})^2 + (z^{(2)} - z_{R_2})^2} \\ \qquad + c \cdot dT_2, \\ p_2^{(3)} = \sqrt{(x^{(3)} - x_{R_2})^2 + (y^{(3)} - y_{R_2})^2 + (z^{(3)} - z_{R_2})^2} \\ \qquad + c \cdot dT_2, \\ p_2^{(4)} = \sqrt{(x^{(4)} - x_{R_2})^2 + (y^{(4)} - y_{R_2})^2 + (z^{(4)} - z_{R_2})^2} \\ \qquad + c \cdot dT_2. \end{cases} \tag{7}$$

From eq. 5, we have

$$\begin{cases} p_1^{(i)} = p^{(i)} + D_1, \\ p_2^{(i)} = p^{(i)} + D_2, \end{cases} \tag{8}$$

for $i = 1, 2, 3, 4$.

Therefore, we can conclude that, for each Satellite i, the difference between $p_1^{(i)}$ (the pseudo range with regard to R_1) and $p_2^{(i)}$ (the pseudo range with regard to R_2) is a constant value $(D_2 - D_1)$.

Then based on eqs. 6 - 8, we have

$$
\begin{cases}
p^{(1)} = \sqrt{(x^{(1)} - x_{R_1})^2 + (y^{(1)} - y_{R_1})^2 + (z^{(1)} - z_{R_1})^2} \\
\quad + c \cdot dT_1 - D_1, \\
\quad = \sqrt{(x^{(1)} - x_{R_2})^2 + (y^{(1)} - y_{R_2})^2 + (z^{(1)} - z_{R_2})^2} \\
\quad + c \cdot dT_2 - D_2, \\
p^{(2)} = \sqrt{(x^{(2)} - x_{R_1})^2 + (y^{(2)} - y_{R_1})^2 + (z^{(2)} - z_{R_1})^2} \\
\quad + c \cdot dT_1 - D_1, \\
\quad = \sqrt{(x^{(2)} - x_{R_2})^2 + (y^{(2)} - y_{R_2})^2 + (z^{(2)} - z_{R_2})^2} \\
\quad + c \cdot dT_2 - D_2, \\
p^{(3)} = \sqrt{(x^{(3)} - x_{R_1})^2 + (y^{(3)} - y_{R_1})^2 + (z^{(3)} - z_{R_1})^2} \\
\quad + c \cdot dT_1 - D_1, \\
\quad = \sqrt{(x^{(3)} - x_{R_2})^2 + (y^{(3)} - y_{R_2})^2 + (z^{(3)} - z_{R_2})^2} \\
\quad + c \cdot dT_2 - D_2, \\
p^{(4)} = \sqrt{(x^{(4)} - x_{R_1})^2 + (y^{(4)} - y_{R_1})^2 + (z^{(4)} - z_{R_1})^2} \\
\quad + c \cdot dT_1 - D_1, \\
\quad = \sqrt{(x^{(4)} - x_{R_2})^2 + (y^{(4)} - y_{R_2})^2 + (z^{(4)} - z_{R_2})^2} \\
\quad + c \cdot dT_2 - D_2.
\end{cases} \tag{9}
$$

Here we can find the solution to the system of eqs. 9 as follows:

$$
\begin{cases}
x_{R_1} = x_{R_2}, \\
y_{R_1} = y_{R_2}, \\
z_{R_1} = z_{R_2}, \\
dT_1 = dT_2 + \dfrac{D_1 - D_2}{c}.
\end{cases} \tag{10}
$$

Therefore, we conclude with the following proposition.

Proposition 1. If we craft spoofed GPS signals using a single spoofer and send them to two (or multiple) GPS receivers in the spoofing area, these GPS receivers will perceive the *same* spoofed location.

This proposition can also be visually explained using Figure. 4. Specifically, trilateration is used by the GPS localization solution. For the single receiver case, we first loosely estimate a large pseudo range p^i for each Satellite i. As the figure shows, at the beginning, the estimated four large pseudo range spheres usually do not intersect at the same point. However, as we gradually decrease the pseudo range estimate p^i for each Satellite i by the same amount little by little, the four pseudo range spheres will eventually intersect at the same point. This point of intersection represents the GPS location solution, and the decrement in pseudo range for each Satellite i is equal to $c \cdot dT$, where dT is the clock offset of the receiver to the GPS system time and c is the speed of light.

Now we go back to the case of two GPS receivers. Based on eq. 8, we have

$$
p_2^{(i)} - p_1^{(i)} = D_2 - D_1, \tag{11}
$$

for $i = 1, 2, 3, 4$.

As we mentioned earlier, eq. 11 means that, for Satellite i, the difference between $p_1^{(i)}$ (the pseudo range with regard to R_1) and $p_2^{(i)}$ (the pseudo range with regard to R_2) is a constant value $(D_2 - D_1)$. Therefore, if we can decrease all pseudo ranges $p_1^{(i)}$ for R_1 by $c \cdot dT_1$ to make the four pseudo range spheres intersect at one location, we can also decrease all pseudo ranges $p_2^{(i)}$ for R_2 by $c \cdot dT_1 + (D_2 - D_1)$ to make the four pseudo range spheres intersect at the same location. This is consistent with eqs. 10. In other words, if we increase or decrease all pseudo ranges for a GPS receiver simultaneously by the same value, the solution of 3D GPS location will not change.

Definition 1. The *same* spoofed location perceived by all the GPS receivers is defined as the *Target Spoofed Location*.

From the aforementioned analysis, we know that the Target Spoofed Location is only determined by $p^{(i)}$ and $(x^{(i)}, y^{(i)}, z^{(i)})$ for $i = 1, 2, 3, 4$, which are used to build the spoofing signals. In the spoofing signal generation procedure, the GPS-SDR-SIM will adjust the spoofing signals such that the Target Spoofed Location at each time step corresponds to the one in the given intended location file.

The Proposition 1 also holds in the case when the GPS receiver tracks more than four satellites. For detailed proof, please refer to our technical report [15].

IV. Performance Evaluation

In the previous section, we have presented the detailed analysis of the location solutions of multiple GPS receivers, given the spoofing signals from a single spoofer. In the following, we will validate the analysis results using experiments with off-the-shelf devices and real GPS data.

A. Hardware and Software Platform

In this section, we will briefly introduce the hardware and software used in the experiments for validating the analysis results.

1) Hardware: **SDR Devices.** In our experiments, we use the low-cost *Nuand bladeRF 2.0* [16] to transmit GPS signals. As the clock precision is not ideal on bladeRF, we also use the *Leobodnar's Precision GPS Reference Clock* [17] as the external clock to make the bladeRF achieve better signal quality and accuracy.

GPS Receivers. In these experiments, we use popular USB-Serial GPS receivers from *Prolific Technology Inc.* [18], and we use *gpsd* [19] as the driver to read the results from the receivers. The *gpsd* allows us to monitor the progress of the experiments, e.g., checking the number of satellites that the receiver is locking to and pseudo-ranges to satellites, and other information.

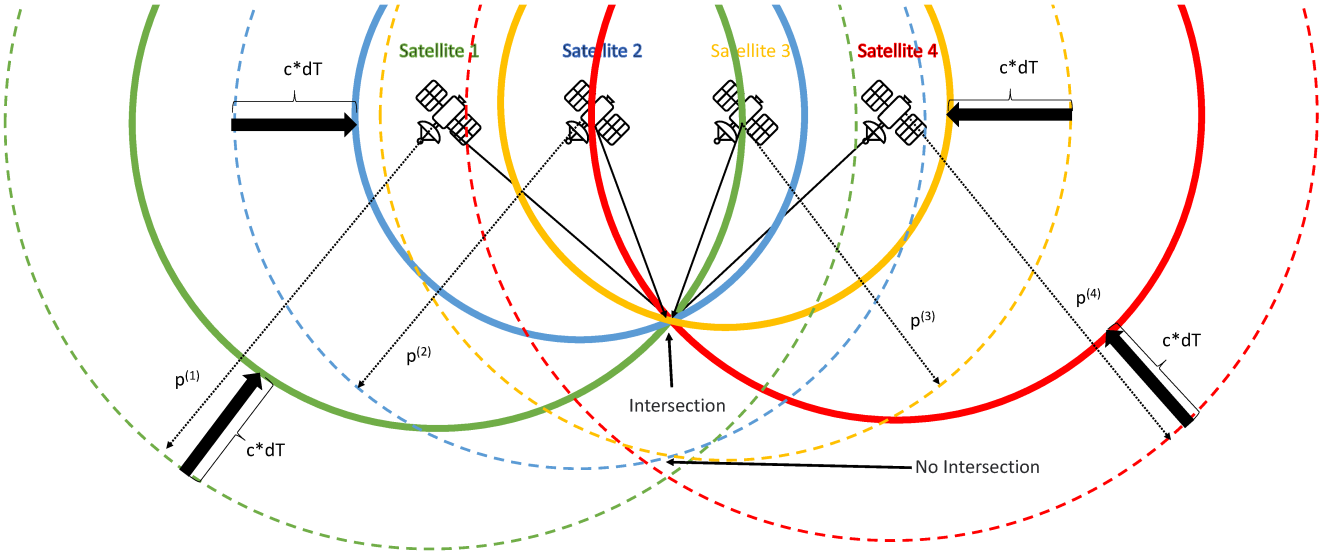

Fig. 4: Visual Explanation of Proposition 1.

2) SDR Software: bladeGPS is an open-source C-based GPS signal generator. It integrates the two tools - *GPS-SDR-SIM* and *bladeRF-cli* that allow us to retrieve the GPS satellite ephemeris from a RINEX file, generates GPS signals for all 32 GPS satellites, and then broadcasts these signals using a bladeRF front end.

NMEA File Generation. For each experiment, we need to input intended spoofing locations to the enhanced bladeGPS to generate spoofing GPS signals. We use a Python script to generate the intended location file in the NMEA format with given parameters, such as GPS signal update rate, initial location, attack duration, spoofing velocity, spoofing direction, etc. For example, we can set the GPS signal update rate at 10 *Hz*, and the initial location at the spoofer's location, the attack duration to 50 *seconds*, a velocity at 1 *m/s* to the North.

B. Experiment Design

In the experiments, we like to validate the correctness of Proposition 1 in different settings. We mostly use two GPS receivers in the experiments. Given that any two receivers at different positions will receive the same spoofed location, for the case of more than two receivers, all receivers in the spoofing area will receive the same location. We vary the experimental settings in terms of (1) spoofing velocity and direction, (2) the distance between the two GPS receivers, and (3) the relative positions between the spoofer and GPS receivers. Therefore, we conduct three sets of experiments corresponding to the above settings. To quantify the consistency among the intended spoofing locations and the resulting spoofed locations observed by the receivers, we use the mean square errors (MSEs) to evaluate the spoofing results. We repeat each experiment many times and use the mean of the results for accuracy.

In all experiments, we use one spoofer and two GPS receivers. For the three sets of experiments, we set the initial spoofing location starting at the spoofer's location, the GPS signal update rate at 10 *Hz*, and the duration of the spoofing GPS signals as 50 *seconds*. In the first 10 *seconds* of the spoofing signals, the spoofing locations remain stationary; after the 10th second, we move the intended spoofing location at a constant velocity in a given direction. For Experiment 1 and Experiment 2, the spoofer is located at the same location as GPS Receiver 1. In addition, for Experiment 1 and Experiment 3, the distance between two GPS receivers is set to 15 meters. Moreover, for Experiment 2 and Experiment 3, the intended spoofing locations are set to move at a velocity of 1 *m/s* to the North. Lastly, the ephemeris files for spoofing are obtained from NASA for all experiments [14].

TABLE II: MSEs under different spoofing velocities.

Spoofing Velocity (m/s)	0.5	1	1.5	2
MSEs - Spoofer and R_1 (m^2)	1.40	1.86	1.42	0.96
MSEs - Spoofer and R_2 (m^2)	2.22	0.71	3.49	1.99
MSEs - R_1 and R_2 (m^2)	1.43	1.79	1.79	1.02

C. Experiment 1: Results under Different Spoofing Velocities and Directions

In the first set of experiments, we evaluate the differences among the intended spoofing locations and the resulting spoofed locations of two GPS receivers R_1 and R_2, under different spoofing velocities and directions. To evaluate the impacts of the velocities, we fix the spoofing direction to the North; to evaluate the impacts of the spoofing direction, we fix the velocity at 1 m/s. We record the raw data (latitudes and longitudes) of the spoofing locations and the spoofed location readings of R_1 and R_2 before and under the attack, convert the location data in *meters*, plot their location trajectories in a figure, and determine the pairwise MSEs for evaluation. Due to space limitation, we will only show one trajectory figure for each set of experiments for demonstration.

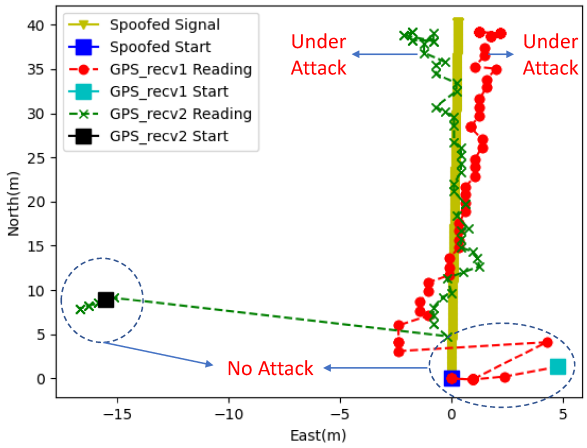

Fig. 5: Three trajectories before and under attack for Experiment 1.

TABLE III: MSEs under different spoofing directions.

Spoofing Direction	N	S	E	W
MSEs - Spoofer and R_1 (m^2)	1.86	0.82	1.51	1.17
MSEs - Spoofer and R_2 (m^2)	0.71	1.63	1.22	2.83
MSEs - R_1 and R_2 (m^2)	1.79	0.35	1.23	0.63

Figure 5 shows the three trajectories under the spoofing signals with a velocity of 1 *m/s* to the North. In this figure, the 2D space represents the locations in a local 2D frame with regard to the initial location of the spoofing signals (i.e., the spoofer location), where the x-axis represents the East direction and y-axis represents the North direction.

From the figure we can easily see that: before attack, the location of the spoofer is at the blue square; the two GPS receivers are at the cyan square and the black square inside the blue ovals. After the attack begins, the readings of R_1 and R_2 will be lost immediately in the first 10 - 20 *seconds*, and then be locked to the spoofing signals. After locked to spoofing signals, their readings jump to very close to the spoofing track, and the three trajectories start to merge and are almost overlapped. The yellowish green is the intended spoofing track, starting with the spoofer's initial location. The red dashed line marked with red dots represents R_1's readings; the green dashed line marked with green-crosses represents R_2's readings.

We also compute the pairwise MSEs of the three trajectories when under attack to quantify their differences. As shown in Table II and Table III, we can find that the MSEs between every two trajectories are all smaller than 3 m^2 under different spoofing velocities and directions, which is well within the typical error ranges of common GPS receivers (within 24 m^2) [20]. Therefore, this set of experiments has showed the correctness of Proposition 1 regardless of spoofing velocities and directions.

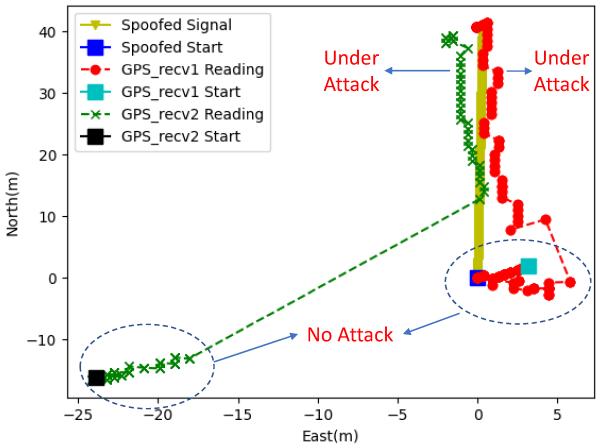

Fig. 6: Three trajectories before and under attack for Experiment 2.

D. Experiment 2: Results under Different Distances between the GPS Receivers

In Experiment 2, we evaluate the differences among the three trajectories under different distances between the two GPS receivers: R_1 and R_2. Figure 6 shows the trajectories of the spoofing track and the readings of R_1 and R_2 before and under attack, when the distance between R_1 and R_2 is 12.5 m. Similarly, this figure shows that the three trajectories are very close under attack. In addition, Table. IV shows the pairwise MSEs among the three trajectories under attack with a variety of distances are all within the typical error ranges of common GPS receivers, which further confirms Proposition 1. Note that here we only increase the distance up to 17.5 m because it reaches the signal coverage capacity of the spoofer we used. This is certainly a limitation of our experiments. We will obtain better devices to confirm the results.

TABLE IV: MSEs under different distances between the GPS receivers.

Distance (m)	10	12.5	15	17.5
MSEs - Spoofer and R_1 (m^2)	1.98	0.44	1.86	2.57
MSEs - Spoofer and R_2 (m^2)	1.34	0.97	0.71	2.32
MSEs - R_1 and R_2 (m^2)	1.33	1.83	1.79	1.83

E. Experiment 3: Results under Different Relative Positions between the Spoofer and the GPS Receivers

In this set of experiments, we record the three trajectories when we change the relative positions between the spoofer and the GPS receivers, and evaluate their similarities. Specifically, we place the spoofer at four different locations relative to the two GPS receivers in this experiment, as shown in Figure 7. Figure 8 illustrates the three trajectories under attack when the spoofer is placed at the relative position of 1/4. Again, we can find that the three trajectories converge after the two GPS receivers are fixed to the spoofing signals. In addition, Table V shows that all pairwise MSEs are within the typical

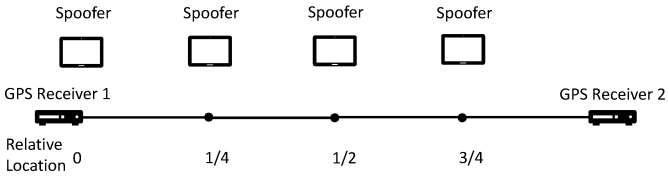

Fig. 7: Settings of spoofer locations in Experiment 3.

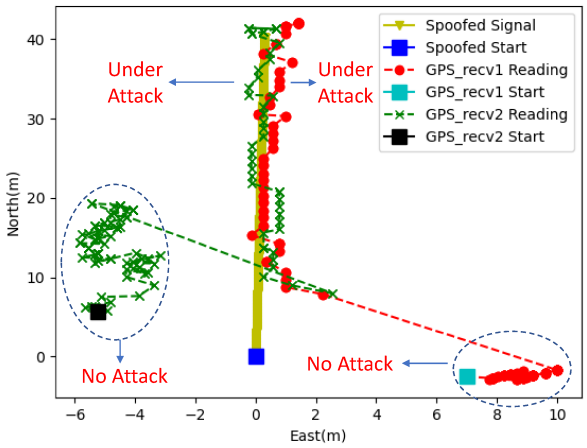

Fig. 8: Three trajectories before and under attack for Experiment 3.

error ranges of common GPS receivers, reaching the same conclusion as the first two sets of experiments. Again, we realize the limitations of these experiments in terms of the distance between the spoofer and the receivers. We will try better devices to increase this distance to further validate our analysis.

TABLE V: MSEs under different relative positions between the spoofer and the GPS receivers.

Spoofer Relative Position	0	1/4	1/2	3/4
MSEs - Spoofer and R_1 (m^2)	1.86	0.68	0.69	2.84
MSEs - Spoofer and R_2 (m^2)	0.71	1.58	1.14	2.59
MSEs - R_1 and R_2 (m^2)	1.79	0.40	0.87	0.24

V. Conclusion and Future Work

In this paper, we investigate the impacts of GPS spoofing with a single spoofer on multiple receivers. We have theoretically proved that when using a single spoofer for GPS spoofing, multiple receivers at different locations within a spoofing area will perceive the same location readings. The correctness of the analysis has been validated with multiple sets of real-world experiments. This result reveals the new threats to multiple mobile devices that rely on GPS, such as drone swarms.

As our future work, we will investigate the challenging case of GPS spoofing with multiple spoofers. There are many interesting theoretical questions to be answered. In addition, combining with GPS spoofing, we will further look into the vulnerabilities of state estimation, navigation control, and cooperation algorithms in autonomous drone swarms, and further develop countermeasures to ensure the safe operations of these systems.

References

[1] T. Humphreys, B. Ledvina, B. O. M.L. Psiaki, and P. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," *https://radionavlab.ae.utexas.edu/images/stories/files/papers/ion2008r01_for_distributionW.pdf*, 2008.

[2] K. Wang, "Time and position spoofing with open source projects," in *BlackHat*, 2015.

[3] K. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1527–1544. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/zeng

[4] J. Gaspar, R. Ferreira, N. Souto, and P. Sebastião, "Capture of uavs through gps spoofing using low-cost sdr platforms," *Wireless Personal Communications*, March 2020.

[5] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful gps spoofing attacks," in *18th ACM conference on Computer and communications security*, 2011.

[6] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[7] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing," *ACM Transactions on Privacy and Security (TOPS)*, vol. 22, no. 2, April 2019.

[8] W. Chen, Y. Dong, and Z. Duan, "DPM: towards accurate drone position manipulation," *IEEE Trans. Dependable Secure Computing*, vol. 20, no. 1, pp. 813–826, 2022. [Online]. Available: https://doi.org/10.1109/TDSC.2022.3144319

[9] A. Annex, "Global positioning system standard positioning service signal specification," *United States Coast Guard Navigation Center*, 1995.

[10] J. A. Volpe, "Vulnerability assessment of the transportation infrastructure relying on global positioning system," Published Date : 2001-08-29. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/8435

[11] B. Motella, M. Pini, M. Fantino, P. Mulassano, M. Nicola, J. Fortuny-Guasch, M. Wildemeersch, and D. Symeonidis, "Performance assessment of low cost gps receivers under civilian spoofing attacks," in *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, 12/2010 2010, pp. 1 –8.

[12] D. He, Y. Qiao, S. Chen, X. Du, W. Chen, S. Zhu, and M. Guizani, "A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles," *IEEE Network*, vol. 33, no. 2, pp. 146–151, 2019.

[13] W. Chen, Y. Dong, and Z. Duan, "Accurately redirecting a malicious drone," in *2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC)*, 2022, pp. 827–834.

[14] NASA. (2023) Broadcast Ephemeris Data. [Online]. Available: https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/broadcast_ephemeris_data.html

[15] W. Chen, Y. Dong, and Z. Duan. (2023) Impacts of a Single GPS Spoofer on Multiple Receivers: Formal Analysis and Experimental Evaluation. [Online]. Available: https://drive.google.com/file/d/1UT74Li3oz8j4AKQNP3RmFd6oBZtpHIdW/view?usp=drive_link

[16] Nuand. (2016) BladeRF wiki. [Online]. Available: https://github.com/nuand/bladeRF/wiki

[17] Leobodnar. (2018) Precision GPS Reference Clock. [Online]. Available: http://www.leobodnar.com/shop/index.php?main_page=product_info&cPath=107&products_id=234

[18] P. T. Inc. (2020) Prolific. [Online]. Available: https://www.prolific.com.tw/US/

[19] GPSD. (2011) gpsd - a GPS service daemon. [Online]. Available: https://gpsd.gitlab.io/gpsd/

[20] N. National Coordination Office for Space-Based Positioning and Timing. (2016) GPS Accuracy. [Online]. Available: https://www.gps.gov/systems/gps/performance/accuracy/