Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications

Christian Sanders and Yongqiang Wang, *Senior Member, IEEE*

***Abstract*—GPS spoofing is a problem that is receiving increasing scrutiny due to an increasing number of reported attacks. Plenty of results have been reported on detecting the presence of GPS spoofing attacks. However, very few results currently exist for the localization of spoofing attackers, which is crucial to counteract GPS attacks. In this paper we propose leveraging vehicle-to-vehicle communications to detect and localize spoofing attacks on vehicular navigation GPS. The key idea is to correlate Doppler shift measurements which are reported by most commercial GPS receivers. The approach does not need additional dedicated devices and is easily deployable on modern vehicles equipped with vehicle-to-vehicle communication devices. It is capable of localizing both stationary spoofers and mobile spoofers which, for example, could be mounted on a vehicle. Both numerical simulations and experimental tests are conducted to confirm the effectiveness of the proposed approach.**

I. Introduction

The global positioning system (GPS) has become a crucial navigation system for all kinds of transportation systems, ranging from planes to ships to cars or even on phones for pedestrians. Furthermore, GPS can also be used for accurate time acquisition, which is crucial for the operation of power systems, banking systems, and stock exchange. Unfortunately, despite being ubiquitous and vital in modern society, GPS is also vulnerable to attacks for a couple of reasons. First, commercial GPS receivers are unable to use encrypted signals from GPS satellites and have to rely on unencrypted messages, which are easy to replicate for an attacker. Also, due to the long distance from GPS satellites to ground GPS receivers, the signals reaching the receivers are extremely weak. In fact, the power of GPS signals received on the Earth is as low as 10^{-16} Watts [1]. Thus, an attacker can easily transmit a stronger signal and drown out the authentic signal.

There are two main types of attacks on GPS receivers: jamming and spoofing. Jamming is the simpler of the two forms, simply involving transmitting noise over GPS frequencies in order to disrupt legitimate signals. This prevents the receiver from calculating its position. Jamming is well understood in the literature [2],[3], and has also been demonstrated numerous times in the real world [4],[5]. Luckily, jamming attacks are typically easy to detect since they cause a receiver to lose a lock, thus revealing their presence to the receiver. On the other hand, a spoofing attack is the process in which an adversary generates and transmits a fake signal in order to fool GPS receivers. As the attacker can force the receiver to believe it is in a different location than it really is, spoofing can allow the attacker to lead the victim off course. Multiple reports have discussed the dangers of this form of attack, which can include severe consequences such as steering planes into mountains or ships into hijacking traps [6],[7].

GPS spoofing has already been demonstrated in real world scenarios. In one demonstration, researchers were able to successfully spoof a yacht at sea and steer it off course [8],[9]. Even more concernedly, it is believed that in 2011 Iran was able to spoof the GPS in a CIA stealth drone, fooling it into landing in a spot where they could capture it in order to reverse engineer the technology [10]. These and other such incidents [11]-[13] demonstrate the pressing need for security solutions for GPS navigation.

The first step in combating spoofing is detection, which has received substantial attention in the past decade. A literature review of some of the reported results is included in section 2. However, even if spoofing can be detected, there is currently not much that can be done about it. There is no way to regain the true signal, and very little research has been reported on locating the attacker, which would be a first necessary step in ending the spoofing and apprehending the spoofer. For airborne attackers Jansen and coauthors use crowdsourcing in airplanes to localize an attacker [31], which is further improved by [32]. However, this approach relies on dedicated infrastructure, i.e., the OpenSky Network [34], which includes over 700 air traffic communication sensors located all around the world. Such infrastructure unfortunately does not exist for other GPS applications, such as cars.

Yu et al. also attempt to localize an attacker, by using a network of GPS receivers of fixed location, which are typically used for time synchronization in the power grid [33]. However, once again this requires a network of GPS receivers with known locations. In the case of a power grid the receivers are fixed in position, so this is a valid assumption. However, for moving vehicles this method would no longer be applicable.

This paper proposes to localize spoofing attackers on vehicular GPS by correlating Doppler measurements from multiple vehicles connected with vehicle-to-vehicle communications. Given that vehicle-to-vehicle communication radios are commercially available and commercial GPS receivers have the capability to measure incoming signals' frequencies (see table I for some examples), the approach does not require dedicated hardware. Both numerical simulations and hardware tests are performed to confirm the effectiveness of the proposed approach.

The authors are with the Department of Electrical and Computer Engineering,Clemson University, Clemson, SC 29634 USA (e-mail:ctsande@clemson.edu; yongqiw@clemson.edu). The work was supported in part by the National Science Foundation under Grant 1738902.

TABLE I
COMMERCIAL GPS RECEIVERS REPORTING DOPPLER SHIFT

Brand	Device	Cost
U-blox	NEO-M8T	$75 [39]
SkyTraq	NS-RAW	$70 [40]
NVS	RasPiGNSS	$170 [41]
Swift	Piksi Multi GNSS Module	$595 [42]
NovAtel	OEM625S	unknown

II. LITERATURE REVIEW ON DETECTION OF GPS SPOOFING

Numerous approaches have been proposed to detect GPS spoofing. One approach used to thwart GPS spoofing is to make use of cryptograph. For example, a navigation message authentication (NMA) based approach is proposed in [17],[18]. In NMA, the navigation message is encrypted or digitally signed with the intent that a receiver can use this information to observe the origin of the signal it is receiving. Other cryptographic defense approaches such as hidden markers [15] have also been examined. Unfortunately, cryptographic defenses have a few major disadvantages. First, these defenses are still vulnerable to replay attacks, where the attacker records a legitimate signal and broadcasts it with a delay [16],[19]. More importantly, these methods require changes to the GPS legacy system. Due to the static nature of the GPS infrastructure and the long deployment cycles, making changes to the legacy system would be costly and time consuming, and is therefore unlikely to occur in the near future.

Non-cryptographic approaches have also been reported to secure GPS. One non-cryptographic method requires cross-correlation of the P(Y) code with a secure receiver [20],[21],[23]. A high correlation value between the secure and insecure receivers implies that both are receiving the same valid signal. Such correlation based detection can also be performed among several cooperative peers [22]. Unfortunately, this method requires additional high-speed sampling devices to receive raw GPS signals on which the correlation can be performed.

Another method for spoofer detection is SPREE [24]. SPREE is a new form of GPS receiver that uses auxiliary peak tracking to check for similar signals. Since real signals still exist in the presence of a spoofing attack (they are simply overshadowed by the more powerful spoofing signals), the presence of two signals of differing power but similar peaks would indicate the presence of both an authentic signal and a spoofed signal. This would alert the receiver to the presence of a spoofing attack. While this method is quite powerful at detecting attacks, it unfortunately requires hardware upgrades to existing receivers that would be expensive.

Finally, one other option for GPS spoofing detection is to use multiple antennas [25]-[30]. If the attacker is spoofing multiple receivers using only one antenna, all receivers will be spoofed to the same location, which would indicate the presence of an attacker. Even if the attacker uses multiple antennas, having multiple receiving antennas still greatly limits the possible locations from which the attacker can successfully operate, which makes spoofing significantly more difficult. However, this method relies on having multiple receivers with known and fixed relative distances, which is not always feasible.

In summary, while there are several methods available for detecting spoofing, they all tend to require either hardware upgrades or alterations to the legacy GPS system which limits their widespread applications to commercial GPS navigation receivers.

III. PROBLEM STATEMENT

A. Attacker Model

This paper considers an attacker transmitting spoofing signals using an omnidirectional antenna. The attacker can be using any type of spoofing, including meaconing. In this case if multiple targets are spoofed they will lock onto the same spoofing signal, and based on the spoofed signal they will calculate the exact same position [25]. Thus, if multiple vehicles in a network begin reporting the exact same location, that would indicate the presence of a spoofing attack. Once spoofing is detected, attempts to localize the attacker can begin.

This paper considers two main cases: a stationary attacker and a moving attacker. Note that most existing results consider a stationary attacker. We also consider moving attackers where the attacker can place its transmitter in, e.g., a moving vehicle.

In both the stationary attacker case and the moving attacker case the attacker is assumed able to vary the frequency at which it transmits fake GPS signals. In order to transmit a valid GPS signal the attacker must transmit at a frequency within a few hundred Hertz of the standard satellite transmission (roughly 1575.42 MHz) [35]. However, within this range the attacker is assumed to be able to have full control of the frequency at which they can transmit, including the ability to change frequencies in real time. The attacker can add whatever noise they wish to the frequency within this range. There will also be some noise in the actual GPS signal, but as long as the receivers can still maintain a lock such noise is irrelevant.

B. Victim Model

This paper considers a set of moving receivers located on different vehicles. These vehicles travel on the same road and can communicate with each other using V2V communications with a standard bandwidth in the 5.85-5.925 GHz band [36]. Each vehicle can record the frequency of the incoming GPS signal, which is reported by most commercial GPS receivers. Each vehicle also has full knowledge of the speed at which it is going and the distance it has traveled between consecutive measurements of the signal frequency. This is reasonable as a vehicle can get the distance information from its odometer. We do not assume that a vehicle knows its exact location.

Each vehicle uses a standard commercial GPS receiver, which reports incoming signal frequencies. Most existing commercial GPS receivers report such measurements. Note that due to the loss of synchronization between receiver clocks and the genuine GPS clocks, these measurements could be subject to errors. We circumvent such errors by using the relative difference between two consecutive measurements in

the computation, as will be detailed in section 4. Furthermore, each receiver needs to be time synchronized with all of the other receivers. This will happen by definition though, as all receivers will be locked on to the same signal generated by the attacker.

IV. Our Approach

A. Static Spoofer Case

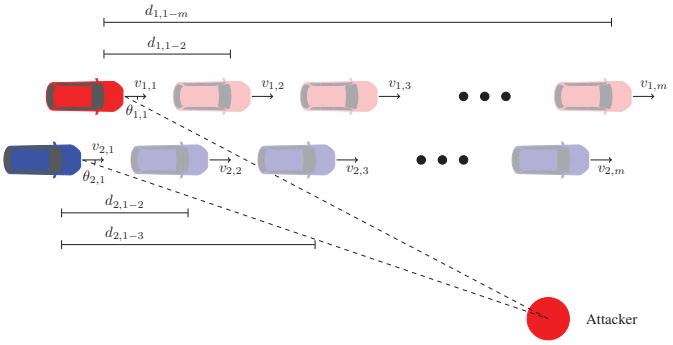

Fig. 1. A diagram of the receivers and the attacker. There are two receivers, 1 and 2, each of which takes measurements at m different instances of measuring time. Each receiver has knowledge of the speed it is moving at each time as well as the distance it has traveled since the first measurement.

Figure 1 shows a schematic of our setup in which we consider $n = 2$ vehicular GPS receivers for the simplicity of exposition. Each receiver takes frequency measurements at m different positions, where m is a positive integer. The receivers will experience some Doppler shift with the signal transmitted from the attacker because of the relative speed between them. Thus, the frequency measured at each point by a given receiver i can be described by the following equation:

$$f = \left(\frac{c + V_i}{c}\right) f_s + \epsilon \tag{1}$$

where f is the measured frequency, f_s is the frequency at which the spoofer transmits signals, V_i is the line of sight velocity of the receiver with respect to the spoofer, c is the speed of light, and ϵ is the error in the receiver. ϵ is caused mainly by the difference in the clocks between the receiver and the GPS satellites. Since it remains almost constant over short time periods it can be eliminated by considering the difference between different samples. For instance, the difference in frequency in receiver i between the first measurement and the jth measurement, where j is some integer between 2 and n, can be represented as follows:

$$\begin{aligned}\Delta f_{i,1-j} &= f_{i,1} - f_{i,j} \\ &= \left(\frac{c + V_{i,1}}{c}\right) f_{s,1} - \left(\frac{c + V_{i,j}}{c}\right) f_{s,j}\end{aligned} \tag{2}$$

As we do not assume that the spoofer is using a constant frequency in signal transmission, we used $f_{s,1}$ and $f_{s,j}$ to denote the respective frequencies at which the spoofing is transmitting when the first and jth measurements were conducted. This equation can be simplified as follows:

$$\Delta f_{i,1-j} = \frac{1}{c}\left(f_{s,1}V_{1,1} - f_{s,j}V_{i,j}\right) + f_{s,1} - f_{s,j} \tag{3}$$

The line of sight velocity of receiver i at time j with respect to the attacker is unknown and can be represented as:

$$V_{i,j} = v_{i,j}\cos(\theta_{i,j}) \tag{4}$$

where $v_{i,j}$ is the speed of receiver i at time j and $\theta_{i,j}$ is the angle between receiver velocity and its direction with respect to the attacker, as illustrated in figure 1. Combining equations (3) and (4) leads to:

$$\begin{aligned}\Delta f_{i,1-j} = \frac{1}{c}\left(f_{s,1}v_{1,1}\cos(\theta_{1,1}) - f_{s,j}v_{i,j}\cos(\theta_{i,j})\right) + \\ f_{s,1} - f_{s,j}\end{aligned} \tag{5}$$

Furthermore, based on the geometry of the formation, $\cos(\theta_{i,j})$ can be represented in terms of variables referencing receiver 1 at the first time sample, described below:

$$\cos(\theta_{i,j}) = \frac{r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j}}{\sqrt{(r_{i,1}\sin(\theta_{i,1}))^2 + (r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})^2}} \tag{6}$$

where $r_{i,1}$ is the distance from receiver i to the attacker when the first measurement was conducted, and $d_{i,1-j}$ is the distance between receiver i's first and jth measurements. This relationship can then be substituted into equation (5), resulting in the following equation:

$$\begin{aligned}\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c}f_{s,1}v_{i,1}\cos(\theta_{i,1}) - \\ \frac{1}{c}\left(\frac{f_{s,1}v_{i,j}(r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})}{\sqrt{(r_{i,1}\sin(\theta_{i,1}))^2 + (r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})^2}}\right)\end{aligned} \tag{7}$$

Equation (7) can be further rewritten as:

$$\begin{aligned}\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c} * \\ \left(f_{s,1}v_{i,1}\cos(\theta_{i,1}) - \frac{f_{s,1}v_{i,j}(r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})}{\sqrt{r_{i,1}^2 + d_{i,1-j}^2 - 2r_{i,1}d_{i,1-j}\cos(\theta_{i,1})}}\right)\end{aligned} \tag{8}$$

Representing $\cos(\theta_{i,1})$ with x_i, equation (8) can be simplified to the following:

$$\begin{aligned}\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \\ \frac{1}{c}\left(f_{s,1}v_{i,1}x_i - \frac{f_{s,1}v_{i,j}(r_{i,1}x_i - d_{i,1-j})}{\sqrt{r_{i,1}^2 + d_{i,1-j}^2 - 2r_{i,1}d_{i,1-j}x_i}}\right)\end{aligned} \tag{9}$$

This same method can be used for every measurement point made by receiver 1, as well as for all other receivers. This

ultimately results in the following system of equations:

$$\begin{cases} \Delta f_{1,1-2} = f_{s,1} - f_{s,2} + \\ \frac{1}{c}\left(f_{s,1}v_{1,1}x_1 - \frac{f_{s,1}v_{1,2}(r_{1,1}x_1 - d_{1,1-2})}{\sqrt{r_{1,t}^2 + d_{1,1-2}^2 - 2r_{1,1}d_{1,1-2}x=1}}\right) \\ \Delta f_{1,1-3} = f_{s,1} - f_{s,3} + \\ \frac{1}{c}\left(f_{s,1}v_{1,1}x_1 - \frac{f_{s,1}v_{1,3}(r_{1,1}x_1 - d_{1,1-3})}{\sqrt{r_{1,t}^2 + d_{1,1-3}^2 - 2r_{1,1}d_{1,1-3}x_1}}\right) \\ \vdots \\ \Delta f_{1,1-m} = f_{s,1} - f_{s,m} + \\ \frac{1}{c}\left(f_{s,1}v_{1,1}x_1 - \frac{f_{s,1}v_{1,m}(r_{1,1}x_1 - d_{1,1-m})}{\sqrt{r_{1,1}^2 + d_{1,1-m}^2 - 2r_{1,1}d_{1,1-m}x_1}}\right) \\ \Delta f_{2,1-2} = f_{s,1} - f_{s,2} + \\ \frac{1}{c}\left(f_{s,1}v_{2,1}x_2 - \frac{f_{s,1}v_{2,2}(r_{2,1}x_2 - d_{2,1-2})}{\sqrt{r_{2,1}^2 + d_{2,1-2}^2 - 2r_{2,1}d_{2,1-2}x_2}}\right) \\ \vdots \\ \Delta f_{2,1-m} = f_{s,1} - f_{s,m} + \\ \frac{1}{c}\left(f_{s,1}v_{2,1}x_2 - \frac{f_{s,1}v_{2,m}(r_{2,1}x_2 - d_{2,1-m})}{\sqrt{r_{2,1}^2 + d_{2,1-m}^2 - 2r_{2,1}d_{2,1-m}x_2}}\right) \\ \vdots \\ \Delta f_{n,1-2} = f_{s,1} - f_{s,2} + \\ \frac{1}{c}\left(f_{s,1}v_{n,1}x_n - \frac{f_{s,1}v_{n,2}(r_{n,1}x_n - d_{n,1})}{\sqrt{r_{n,1}^2 + d_{n,1-2}^2 - 2r_{n,1}d_{n,1-2}x_n}}\right) \\ \vdots \\ \Delta f_{n,1-m} = f_{s,1} - f_{s,m} + \\ \frac{1}{c}\left(f_{s,1}v_{n,1}x_n - \frac{f_{s,1}v_{n,m}(r_{n,1}x_n - d_{n,1})}{\sqrt{r_{n,1}^2 + d_{n,1-m}^2 - 2r_{n,1}d_{n,1-m}x_n}}\right) \end{cases} \tag{10}$$

Suppose there are n receivers, each conducting m measurements, then we can construct $n(m-1)$ equations in (10). In these equations, there are $2n+m$ unknowns, ie. θ for each receiver, r for each receiver, and f_s transmitted at each time instance. Therefore, when m is larger than 6, we have $n(m+1) > 2n+m$, and hence can solve for the unknowns in (10). Using the same argument, we can know that three receivers only require five measurements per receivers and four or more receivers only require four measurements per receiver. However, any number of receivers can take additional measurements per receiver to potentially improve accuracy. As such, once this system of equations is solved, the position of the attacker is known relative to each receiver. Note that since the cosine of an angle can correspond to two different angles, there are two possible solutions. Due to the symmetry of the problem, where Doppler shifts experienced with respect to spoofers on the left of the receiver are indistinguishable from Doppler shifts experienced with respect to spoofers on the right of the receive, it is impossible to narrow it down to only one solution, so both locations would have to be investigated to localize the attacker. This can be seen in figure 2.

The above approach to calculating $r_{i,1}$ and $\theta_{i,1}$ hence obtaining the location of the spoofer is applicable only when the measurements are noise-free. Given that the measurements are always subject to noise, we choose to estimate the location of the spoofer by solving the following optimization problem:

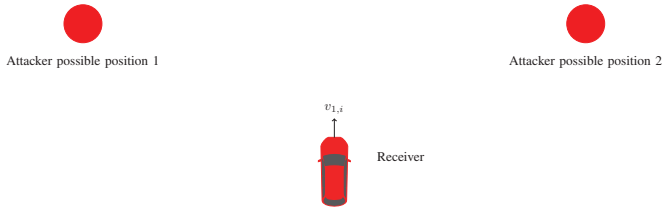

Fig. 2. The receiver receives the same Doppler shift from an attacker located on either side of it. Therefore, each solution will have two possible locations.

$$\begin{aligned} &\min_{X\in\mathbb{R}^d} \sum_{i=1}^{n}\sum_{j=2}^{m} E_{i,j}^2 \\ &X = (\theta_{1,1}, \theta_{2,1}, ..., \theta_{i,1}, r_{1,1}, ..., r_{i,1}, f_{s,1}, ..., f_{s,j}) \end{aligned} \tag{11}$$

where $E_{i,j}$ is the error for car i at sample j, which is the difference between the measure Doppler shift and the Doppler shift calculated based on the chosen parameters or:

$$\begin{aligned} E_{i,j} = \Delta f_{i,1-j} - f_{s,1} - f_{s,j} + \\ \frac{1}{c}\left(f_{s,1}v_{i,1}x - \frac{f_{s,1}v_{i,j}(r_{i,1}x - d_{i,1-j})}{\sqrt{r_{i,1}^2 + d_{i,1-j}^2 - 2r_{i,1}d_{i,1-j}x}}\right) \end{aligned} \tag{12}$$

Solving for (11) gives the optimal solution for this problem.

B. Mobile Spoofer Case

Just like in the stationary spoofer case, in the moving spoofer case we can also calculate the position of an attacker by examining the difference between Doppler shifts at different measurement points. However, in this case the Doppler shift is not only affected by the motion of the receivers but also by the unknown motion of the attacker. Therefore, the difference in Doppler shifts between two measurement points can be characterized by the following equation for receiver i:

$$\begin{aligned} \Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \\ \frac{1}{c}\left(f_{s,1}(V_{i,1} + V_{s,1}) - f_{s,j}(V_{i,j} + V_{s,j})\right) \end{aligned} \tag{13}$$

where $V_{i,1}$ and $V_{i,j}$ are the line of sight velocities of the victim with respect to the spoofer when conducting the first and jth measurements respectively and $V_{s,1}$ and $V_{s,j}$ are the line of sight velocities of the spoofer when the first and jth measurement were conducted by receiver i, respectively.

Just like in the stationary spoofer case, the line of sight velocities are not known. So we represent it as follows:

$$V_{i,j} = v_{i,j}\cos(\theta_{i,j}) \tag{14}$$

where $v_{i,j}$ is the magnitude of the velocity of the victim, which is known to vehicle i, and $\theta_{i,j}$ is the angle that vehicle i's velocity makes with the direction to the spoofer.

All line of sight victim velocities at future times can also be represented in terms of $\theta_{i,1}$. Based on the geometry of the problem, $\cos(\theta_{i,j})$ can be represented as follows:

$$\cos(\theta_{i,j}) = \frac{r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j} + T * v_s\cos(\theta_s)}{\sqrt{r_{y,i,j}^2 + r_{x,i,j}^2}} \tag{15}$$

where

$$r_{y,i,j} = r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j} + (i-1)T * v_s\cos(\theta_s) \quad (16)$$

and

$$r_{x,i,j} = r_{i,1}\sin(\theta_{i,1}) + (i-1)T * v_s\sin(\theta_s) \quad (17)$$

Here, T is the sampling period of the receiver.

In order to represent the attack motion's influence on the measured Doppler shift a similar process can be completed. Once again, the velocity of the spoofer can be multiplied by the cosine of the angle it makes with the receiver. However, since the angle the attacker's velocity makes with each victim is constantly changing, it cannot be represented as a single variable and must therefore be defined by multiple other variables for each time instant. For instance, the angle that the velocity of the spoofer makes with receiver i at the jth time instant can be represented as:

$$\theta_{s,i,j} = \theta_s + \pi - \theta_{i,j} \quad (18)$$

where $\theta_{s,i,j}$ is the angle that the spoofer's velocity makes with receiver i at time j and θ_s is the angle the attacker's velocity makes with the victims' direction of motion, which is assumed to be the same during vehicle i's m samples.

Furthermore, the angle the velocity of the spoofer makes with receiver i at other time instants can be represented in terms of variables from the first time instant, as can be seen below for the jth time sample:

$$\theta_{s,i,j} = \theta_s + \pi - \cos^{-1}(\cos(\theta_{i,j})) \quad (19)$$

where $\cos(\theta_{i,j})$ can be represented as demonstrated in equation (15).

Therefore, equations (14) through (19) can be substituted into equation (13) to produce the following equation:

$$\begin{aligned}&\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \\ &\frac{1}{c}(f_{s,1}(v_{i,1}cos(\theta_{i,1}) + v_s\cos(\theta_s + 180 - \theta_{i,j})) - f_{s,j} * \\ &(v_{i,j}\cos(\theta_{i,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{i,j}))))\end{aligned} \quad (20)$$

A similar equation can be created for each receiver at each sample after the first. This results in the following system of equations:

$$\begin{cases}\begin{aligned}&\Delta f_{1,1-2} = f_{s,1} - f_{s,2} + \\ &\tfrac{1}{c}(f_{s,1}(v_{1,1}cos(\theta_{1,1}) + v_s\cos(\theta_s + \pi - \theta_{1,1})) - f_{s,2} * \\ &(v_{1,2}\cos(\theta_{1,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{1,2})))))\end{aligned} \\ \begin{aligned}&\Delta f_{1,1-3} = f_{s,1} - f_{s,3} + \\ &\tfrac{1}{c}(f_{s,1}(v_{1,1}cos(\theta_{1,1}) + v_s\cos(\theta_s + \pi - \theta_{1,1})) - f_{s,3} * \\ &(v_{1,3}\cos(\theta_{1,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{1,3})))))\end{aligned} \\ \vdots \\ \begin{aligned}&\Delta f_{1,1-m} = f_{s,1} - f_{s,m} + \\ &\tfrac{1}{c}(f_{s,1}(v_{1,1}cos(\theta_{1,1}) + v_s\cos(\theta_s + \pi - \theta_{1,1})) - f_{s,m} * \\ &(v_{1,m}\cos(\theta_{1,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{1,m})))))\end{aligned} \\ \begin{aligned}&\Delta f_{2,1-2} = f_{s,1} - f_{s,2} + \\ &\tfrac{1}{c}(f_{s,1}(v_{2,1}cos(\theta_{2,1}) + v_s\cos(\theta_s + \pi - \theta_{2,1})) - f_{s,2} * \\ &(v_{2,2}\cos(\theta_{2,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{2,2})))))\end{aligned} \\ \vdots \\ \begin{aligned}&\Delta f_{2,1-m} = f_{s,1} - f_{s,m} + \\ &\tfrac{1}{c}(f_{s,1}(v_{2,1}cos(\theta_{2,1}) + v_s\cos(\theta_s + \pi - \theta_{2,1})) - f_{s,m} * \\ &(v_{2,m}\cos(\theta_{2,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{2,m})))))\end{aligned} \\ \vdots \\ \begin{aligned}&\Delta f_{n,1-2} = f_{s,1} - f_{s,2} + \\ &\tfrac{1}{c}(f_{s,1}(v_{n,1}cos(\theta_{n,1}) + v_s\cos(\theta_s + \pi - \theta_{n,1})) - f_{s,2} * \\ &(v_{n,2}\cos(\theta_{n,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{n,2})))))\end{aligned} \\ \vdots \\ \begin{aligned}&\Delta f_{n,1-m} = f_{s,1} - f_{s,m} + \\ &\tfrac{1}{c}(f_{s,1}(v_{n,1}cos(\theta_{n,1}) + v_s\cos(\theta_s + \pi - \theta_{n,1})) - f_{s,m} * \\ &(v_{n,m}\cos(\theta_{n,1}) + v_s\cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{n,m})))))\end{aligned}\end{cases} \quad (21)$$

Once again, suppose there are n receivers, each conducting m measurements. This allows us to construct $n(m-1)$ equations in (21). In these equations there are $2n+m+2$ unknowns, which once again include θ for each receiver, r for each receiver, and the transmitted frequency, f_s, at each time instant. However, in this case the spoofer also has an unknown speed, v_s, and direction, θ_s. Thus, when n is 3 and m is 6, we have $n(m-1) > 2n+m+2$, and can thus solve for the unknowns. Using the same argument, we can say that as the number of receivers increases the number of required measurements decreases. However, any number of receivers can still take additional measurements to potentially improve accuracy. Therefore, once this system is solved, the position of the attacker is known relative to each receiver and the speed and direction of the attacker is also obtained. Note that once again the symmetry of the problem leads to two potential solutions, which would both need to be investigated.

Similarly to the stationary case, noise in the system prevents it from finding an actual solution. Therefore, once again it is necessary to minimize localization error based on the following optimization problem:

$$\begin{aligned}&\min_{X\in\mathbb{R}^d} \sum_{i=1}^{n}\sum_{j=2}^{m} E_{i,j}^2 \\ &X = (\theta_{1,1}, \theta_{2,1}, ..., \theta_{i,1}, r_{1,1}, ..., r_{i,1}, f_{s,1}, ..., f_{s,j}, v_s, \theta_s)\end{aligned} \quad (22)$$

where $E_{i,j}$ is the error between the measured Doppler shift and the Doppler shift calculated based on parameters, as demonstrated below:

$$E_{i,j} = \Delta f_{i,1-j} - f_{s,1} - f_{s,j} + \frac{1}{c}(f_{s,1}(v_{i,1}cos(\theta_{i,1}) + v_s \cos(\theta_s + \pi - \theta_{i,1})) - f_{s,j}(v_{i,j}\cos(\theta_{i,1}) + v_s \cos(\theta_s + \pi - \cos^{-1}(cos(\theta_{i,j})))))) \quad (23)$$

V. Evaluation Based on Numerical Simulations

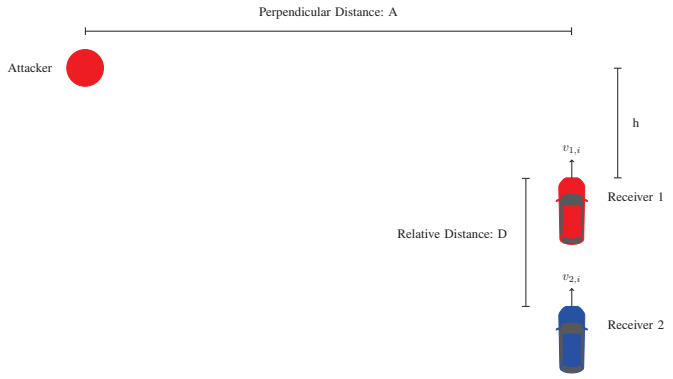

Fig. 3. A diagram of the spoofer setup used in numerical simulations.

We first conducted numerical simulations to verify the effectiveness of our attack localization approach.

In the simulation we assume that all vehicles travel along the same road with the same constant speed, ie. $v_{1,j} = v_{2,j}$, 20 m/s, as illustrated in figure 3. This setting involves three parameters, the relative distances between consecutive receivers (D), the perpendicular distance from the attacker to the receivers (A), and the parallel distance from the front vehicle to the attacker (h). We systematically evaluated the influence of these parameters as well as the number of samples/cars to the localization performance. Table II displays the variables examined and the corresponding figures.

TABLE II
A Summary of Different Cases Considered in the Simulation/Validation

	Stationary Spoofer	**Moving Spoofer**
Influence of number of samples	Figure 4	Figure 7, Figure 8
Influence of h	Figure 9	Figure 10
Influence of A	Figure 11	Figure 12
Influence of D	Figure 13	Figure 14

Setting D equal to 10 meters, A equal to 100 meters, and h equal to 145 meters, we first evaluated the performance of the algorithm under different number of samples. To emulate measurement noise we add Gaussian noise with standard deviation of .05. This amount of noise was chosen because it was large enough to prevent the system of equations to be solved precisely but small enough to not obscure the trends present in the algorithm. We considered 3 cases with the number of vehicle receivers set to 2, 3, and 4 respectively. Each vehicle recorded a measurement every three seconds. The errors of localization for the three cases with different numbers of samples are illustrated in figure 4. In the figure, we run each test for 100 runs. Note that in the 2-car case no data is given when the number of samples is 5, as in this case the number of samples is not enough to arrive at a solution. Each vehicle recorded a measurement every three seconds and calculated the position of the attacker. The errors (discrepancy between the calculated position and the real position) on relevant vehicles were averaged together and used to measure the localization performance.

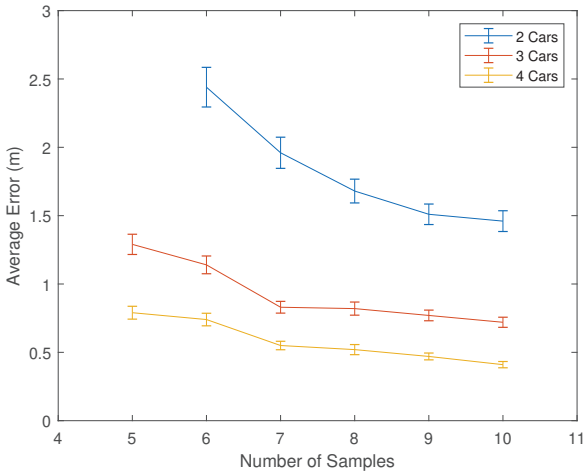

Fig. 4. The influence of the number of samples (m) on localization performance in the static spoofer case.

It can be seen that as the number of samples increases the average error consistently decreases. This was expected as additional data should allow for more accurate calculations. Furthermore, as the number of vehicles increased the average error also decreased.

Similar simulations were carried out for the mobile spoofer case. Samples were still collected every three seconds by each vehicle and Gaussian noise was assumed to have a standard deviation of .05.

These simulations were conducted for two different formations of moving spoofers: one where the spoofer is moving at a 45 degree angle relative to the receivers (figure 5) and one where the spoofer is on the same road as the receivers but traveling in the opposite direction (figure 6). In both formations, all victims were assumed to be on the same road driving in the same direction. In figure 6 the perpendicular distance, A, is set to 5 meters to reflect the distance to the other side of the road. Furthermore, the spoofer and the receivers are all moving at the same speed, 20 m/s.

Figure 7 displays the localization error in the first formation. Once again, it can be seen that the localization becomes more accurate with additional samples and vehicles. A similar simulation was conducted for the second formation, as illustrated in figure 8. However, in this case it can be seen that increased numbers of samples had no effect on the localization accuracy.

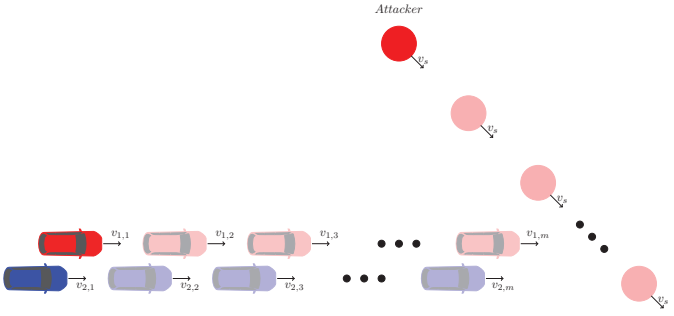

Fig. 5. A diagram of the formation examined where the attacker moves at a 45 degree angle with the receivers. Only two receivers are shown here due to space constraints.

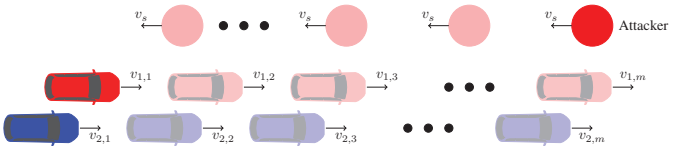

Fig. 6. A diagram of the formation of the receivers moving in the opposite direction of the attacker on the same road.

Figure 8 shows the results for the three car case, but the four and five car plots are identical, revealing that an increased number of vehicles also has no effect on localization accuracy under these conditions. This is reasonable because the only change in Doppler shift occurs when a vehicle passes the spoofer, so adding additional measurements at other points does not actually lead to additional useful information.

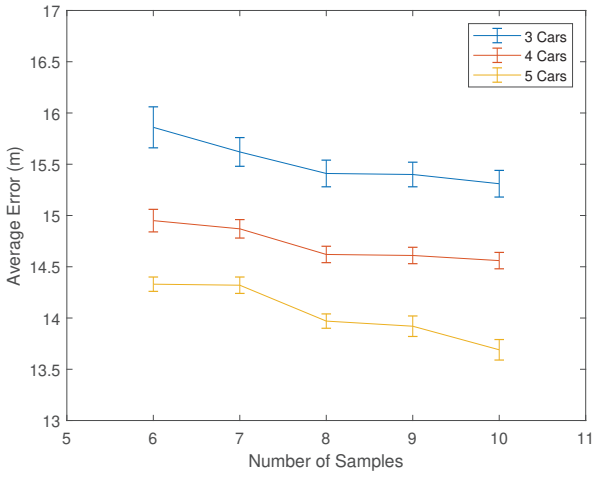

Fig. 7. The influence of the number of samples (m) on localization performance in the moving spoofer case illustrated in figure 5.

We also evaluated the influence of h, the parallel distance from the front vehicle to the attacker, on the localization performance in figure 9. As can be seen, the error starts fairly high for low values of h before decreasing, staying relatively constant for some time, and then increasing again. If h continues to increase past the plotted values, the error increases far more dramatically. This trend holds true for

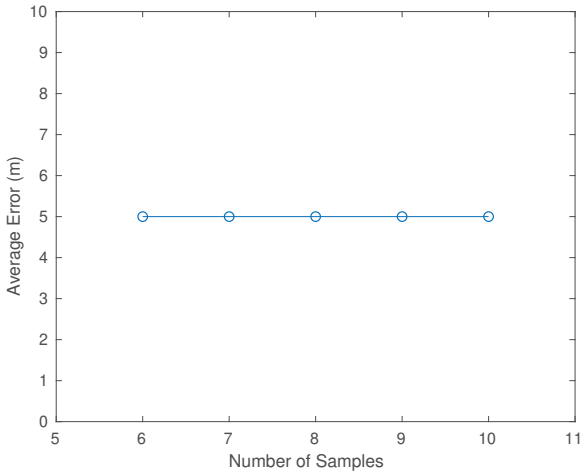

Fig. 8. The influence of the number of samples (m) on localization performance in the moving spoofer case illustrated in figure 6.

different numbers of vehicles and indicates that this method is most accurate when the receivers pass the attacker during conducting measurements, thus creating the widest range of angles with respect to the attacker throughout the measurements. At very low or high values of h, the receivers spend almost the entire time either driving towards or away from the attacker, and thus the range of angles is at most 90 degrees. However, at the middle values of h the receivers pass the attacker and can have a range of angles up to 180 degrees. Since the Doppler shift is directly related to the angle the receiver makes with the attacker, a greater range of angles will lead to a greater range in changing Doppler shifts and thus improved accuracy.

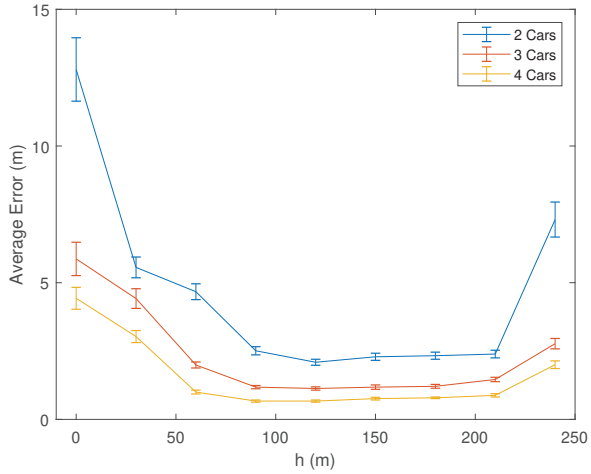

Fig. 9. The influence of the distance h on the localization performance for the static spoofer case.

The effect of changing h was also evaluated in the moving case illustrated in figure 5, as can be seen in figure 10. Similarly to the stationary spoofer case, the error at first decreases with increasing h and then begins to increase again.

Once again, this demonstrates that our method is most effective where the receivers cross the spoofer.

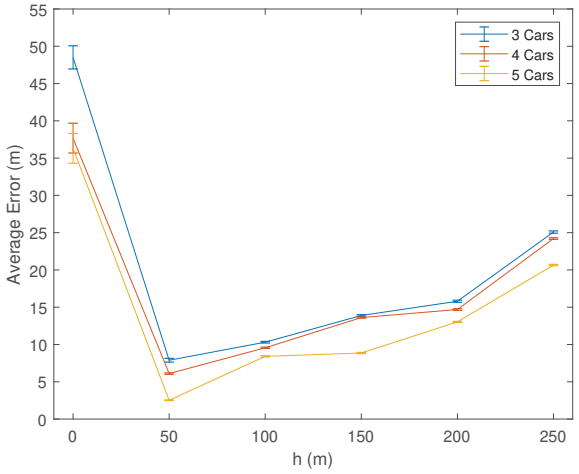

Fig. 10. The influence of the distance h on the localization performance for the moving spoofer case illustrated in figure 5.

The effect of the attacker distance, A, was also evaluated for both the stationary and moving spoofer cases. Figure 11 displays the effect of A in the stationary case. In general, as A increases so does the calculated error. However, if A is too low, such as when it is equal to 10 meters, the error is also high.

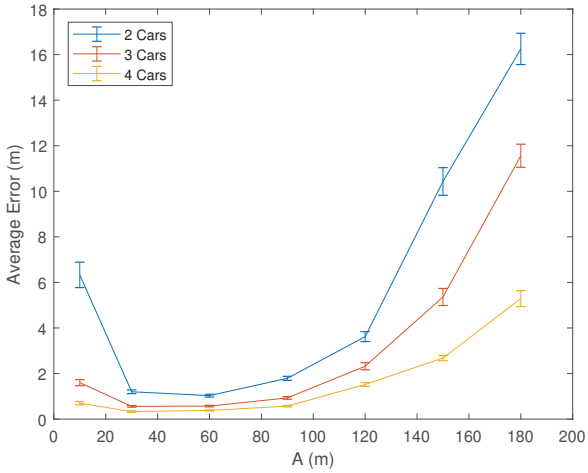

Fig. 11. The influence of the attacker distance, A, on the localization performance in the static spoofer case.

Figure 12 demonstrates the effect of changing A in the 45 degree moving attacker case. Just like in the stationary case, as A increases so does the calculated error.

Finally, simulations were conducted to evaluate the influence of D, the relative distance between receivers. Figure 13 displays the average error with changing D for the stationary spoofer case. As can be seen, the error generally decreases as D increases, which makes sense because at greater values for D the Doppler shift is more different for different receivers.

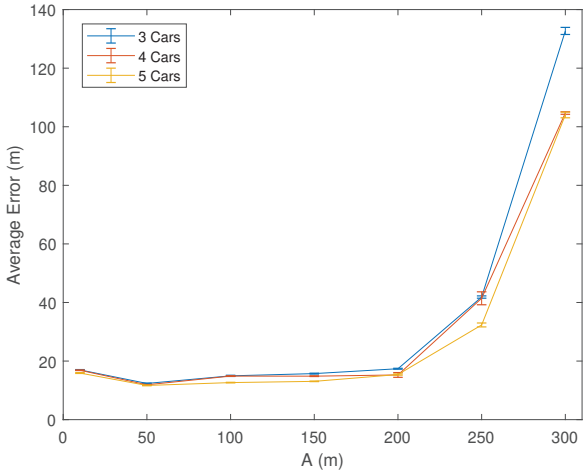

Fig. 12. The influence of the attacker distance, A, on the localization performance for the moving spoofer case illustrated in figure 5.

However, after a distance of 60 meters, the average error increases dramatically, to as much as several hundred meters of error. This is not shown in figure 13 as the difference in error will obscure the trends in the first 60 meters. This effect is most pronounced with more receivers due to the fact that with more receivers the distance from the front receiver to the back receiver is greatly affected by the distance between each receiver. Therefore, once the back receiver gets too far away the method is no longer able to function effectively.

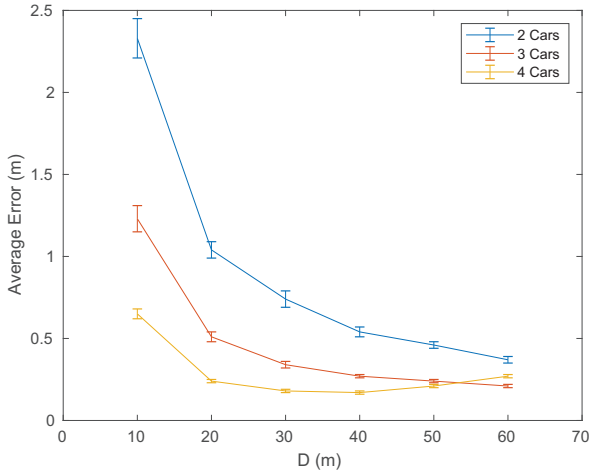

Fig. 13. The influence of the relative receiver distance, D, on localization performance for the static spoofer case.

Figure 14 displays the effect of changing D in the moving spoofer case illustrated in figure 5. Unlike the stationary case, the error in the moving case increases fairly consistently with an increase in D. Thus, the moving spoofer case is most accurate at low relative distances between receivers. This is because the numerical solver used to localize the spoofer in the moving system assumes that $\theta_{i,1}$ is very similar for each receiver. As D increases, this is no longer true, especially with

additional receivers, so the solver is no longer able to reach an accurate solution. As such, this method is only effective to localize moving attackers when distances between receivers are small.

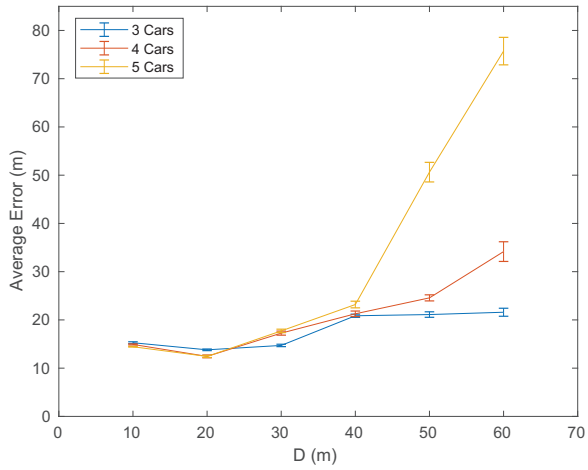

Fig. 14. The influence of the relative receiver distance, D, on localization performance for the moving spoofer case.

VI. Evaluation Based on Experiments

In order to evaluate the effectiveness of this method in a more realistic scenario, hardware experiments were also conducted. Unfortunately, due to laws prohibiting spoofing in the open, we hard-wired the spoofer and GPS receiver and used aluminum shielding to prevent any signal leakage. To emulate the influence of Doppler shift due to the relative movement between the receiver and spoofer, we hard coded the calculated Doppler shift into the spoofer signal.

The USRP B210 from Ettus Research was used as the spoofing device which can transmit signals simultaneously over two channels. The spoofing was accomplished using the gps-sdr-sim spoofing library [38], which can be found publicly online. This library can be used to transmit a spoofing signal to any predetermined location. In this experiment it was simply transmitted with an overall frequency offset in order to represent the Doppler shift.

The receivers used in this experiment were the NEO-M8T Ublox receivers. These receivers have capabilities comparable to most standard commercial receivers. The basic experimental setup is diagrammed in figure 15.

After the frequencies were obtained at each measurement point they were processed using Matlab.

We first evaluated the influence of perpendicular distance (A) and receiver relative distance (D) on the localization performance, with results illustrated in figure 16. In this experiment, all vehicles traveled at 20 m/s and had a parallel distance, h, of 150 meters.

As can be seen in the plot, the localization error first decreases with an increase in the distance from the spoofer (A), but then increases with an increase in A. This is consistent with the numerical simulation results in figure 11.

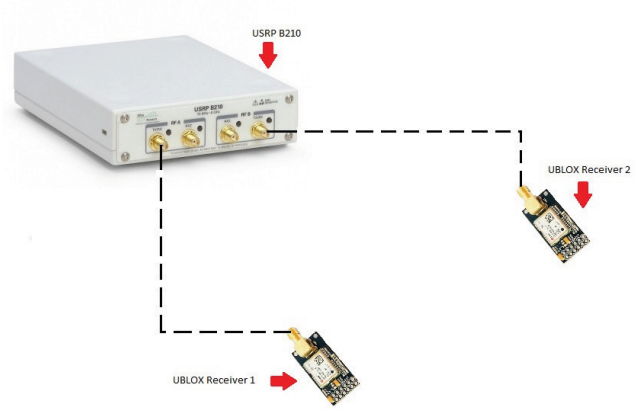

Fig. 15. A diagram of the basic experimental setup. The USRP B210 simultaneously transmits signals over two channels to two separate GPS receivers. These would be shielded in aluminum to prevent signal leakage.

We also evaluated the influence of relative distance between vehicles, D, on the localization performance. The results are given in figure 17. This demonstrates the patterns found in changing distances in between receivers. As can be seen, the general trend is fairly consistent regardless of distance from the attacker. More specifically, the localization error first decreases and then increases with an increase in the relative distance, which is consistent with the numerical simulation results in figure 13.

VII. Discussions

Now we discuss the potential influence of V2X communication imperfections on the performance of our approach. The method will not be affected by potential clock errors between communicating V2X devices. This is because when spoofing occurs, all affected receivers will be locked onto the same spoofing signal, which will guarantee synchronized internal clocks and hence aligned timestamps across communicating V2X devices. The fact that the same spoofing signal synchronizes relevant V2X devices also makes latencies in V2X communications irrelevant to our method because our localization calculations do not have to occur in real time, and only take place after enough measurements are recorded. The fact that the time stamps are synchronized should be sufficient for the correct implementation of the method. Following the same argument, no matter what GPS model a GPS spoofer uses, it has to guarantee that its signal can be locked onto by a GPS receiver, because otherwise it is impossible to mount a successful spoofing attack. Once locked onto the spoofing signal, receiving GPS receivers can always use our approach to detect the presence of a spoofing attack, calculate Doppler shift values, and hence conduct spoofer localization. Therefore, our localization approach is not affected by the GPS signal model used by the attacker (in launching spoofing attacks) or the signal model used by the receiver (in calculating position and time fixes).

It is possible that packet losses in V2X communications may affect the performance of our approach. Therefore, we

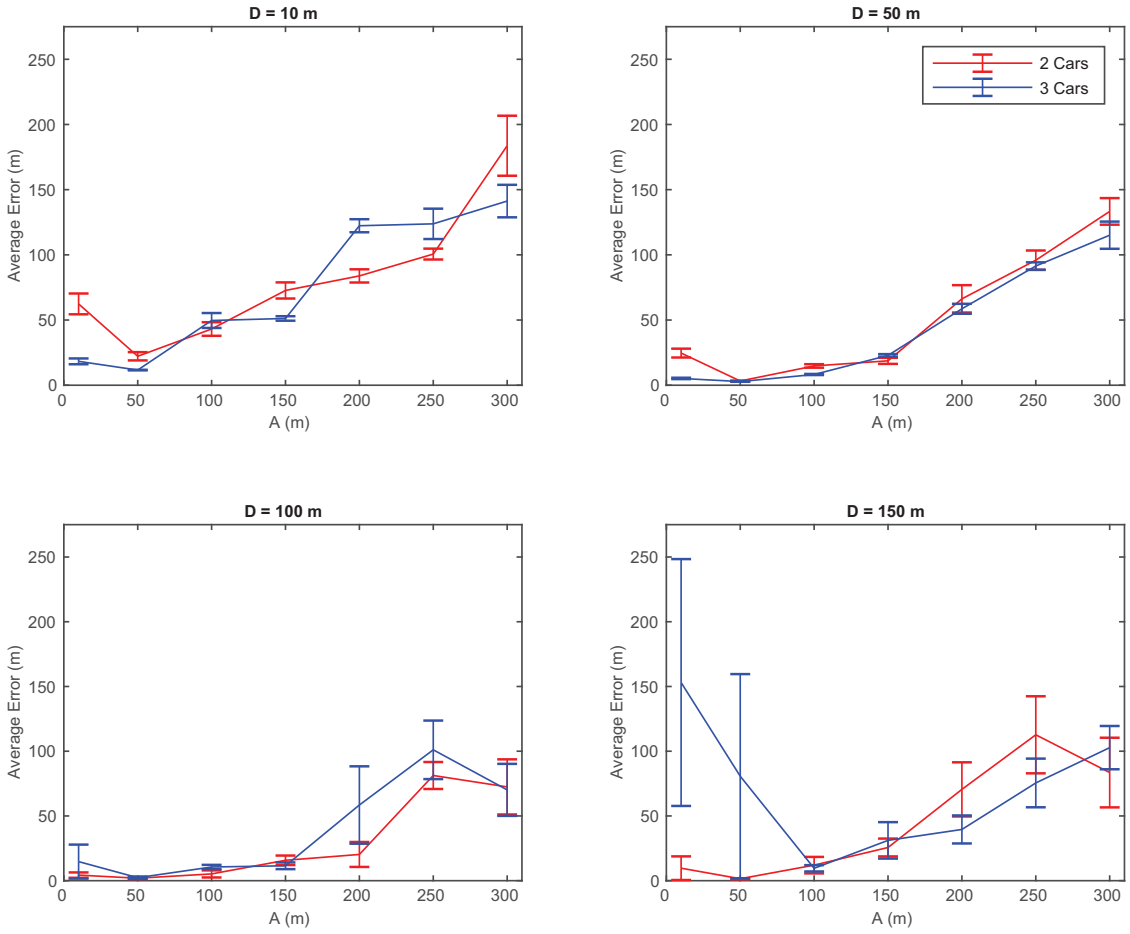

Fig. 16. The average calculation error at different distances from the attacker and different relative vehicle distances.

evaluated the robustness of our approach against message losses. As when a message with a certain timestamp is lost, the receiving device has to discard its measurements with the same timestamp and wait for measurement conducted at the next time instant, the influence of message loss amounts to making the sampling period time-varying. Figure 18 demonstrates the result of conducting the simulation from figure 4 under a random sampling period uniformly distributed between 1 and 5 seconds instead of a fixed sampling period of 3 seconds. As can be seen, while there is slightly larger error than in figure 4, the general trends remain the same. This indicates that as long as enough measurements are properly recorded, message losses occurred in V2X communications do not affect the performance of our approach. Similar tests were carried out for other simulations, but we did not include the results here since all results are very similar.

Finally, it is worth noting that our approach only requires exchanging frequency measurement, speed, and distance travelled among communicating vehicles on the frequency level of once every three seconds. Therefore, the communication overhead is easily manageable for V2X communications which are designed with transmitting period on the order of millisecond [43].

This method could be further applied to a rescue scenario. If a car loses access to the GPS signal and needs to reestablish its location it can begin broadcasting a signal of known frequency. This frequency would not be in the same frequency band as GPS signals to avoid interference, but other vehicles in the vicinity would be able to receive it, calculate the position of the lost vehicle based on measured Doppler shift, and send calculated position to the lost vehicle.

VIII. Conclusion

In this paper we propose using a network of cooperative vehicles to localize a spoofing attacker through use of their respective Doppler shifts. To our knowledge, this is the first time localization of GPS spoofers is addressed for navigation GPS in cars. The effectiveness of the results were evaluated using both numerical simulations and hardware experiments.

This method can be generalized in a few ways. First, in this paper it is assumed that all vehicles move in a perfectly straight line. This is reasonable as vehicle traveling directions will not

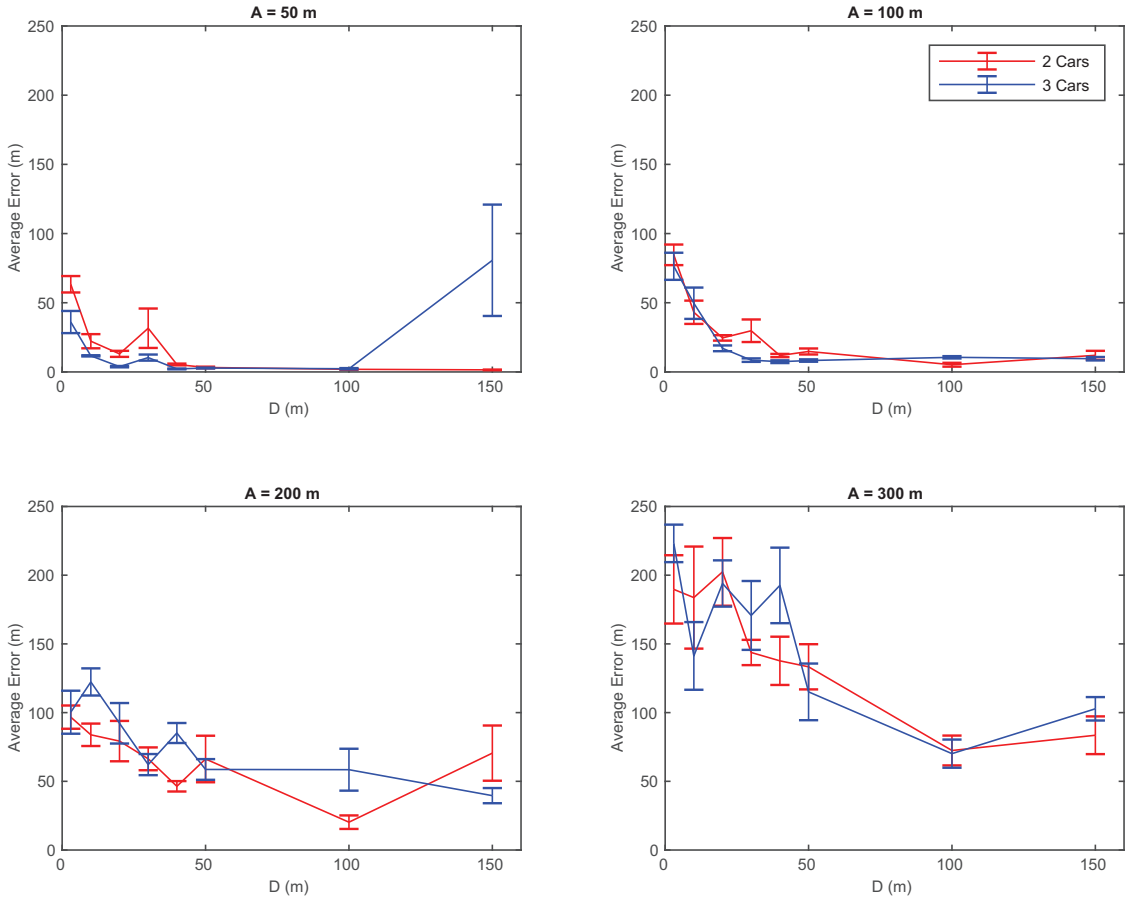

Fig. 17. The average calculation error at different perpendicular distances from the attacker and different relative vehicle distances.

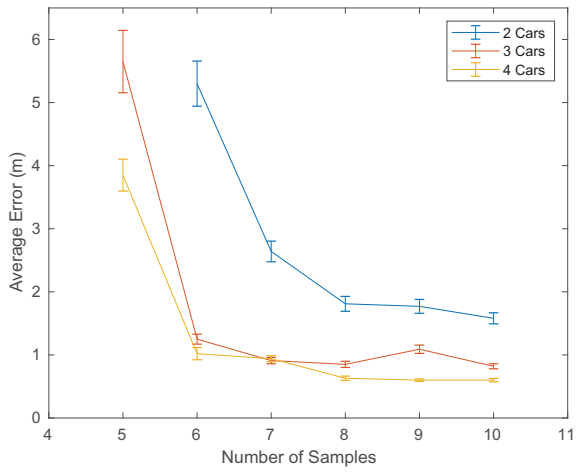

Fig. 18. Average error under different numbers of samples when the sampling period randomly varied uniformly between 1 and 5 seconds.

change dramatically in a short sampling period. In a real world scenario where receivers are constantly sampling, there will be many sampling periods where the spoofer does move in this manner. Therefore, as long as the receivers continue sampling over multiple periods localization should still be possible. In the future, we plan to consider vehicles traveling on curves with turning angles accessible to individual vehicles. In this case, as Doppler shifts will vary with more versatile patterns, we might be able to obtain improved localization performance.

Furthermore, an attacker can attempt to reduce the number of cars affected by its signal by spoofing in low traffic areas or using a directional antenna. This still does not completely rule out the possibility of detection and localization though. They can also circumvent this method by spoofing from multiple antennas, although doing this for a moving victim could prove very difficult [25].

REFERENCES

[1] P. Misra, P. Enge, Global Positioning System: Signals Measurements and Performance, Lincoln, MA, USA:Ganga-Jamuna Press, 2006.

[2] U. Hunkeler, J. Colli-Vignarelli, C. Dehollain, “Effectiveness of GPS-jamming and counter-measures”, Proc. Int. Conf. Localization GNSS, pp. 1-4, 2012.

[3] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS Software Attacks," in ACM Conference on Computer and Communications Security, CCS'12. Raleigh, NC, USA: ACM, Oct. 2012, pp. 450–461.

[4] D. Namowitz. (202, January) "GPS Jamming Expected in Southeast During Military Exercise" [Online]. Available: https://www.aopa.org/news-and-media/all-news/2020/january/14/gps-jamming-expected-in-southeast-during-military-exercise

[5] Massive GPS Jamming Attack by North Korea (2012, May) [Online]. Available: https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/

[6] Anon., "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," John A. Volpe National Transportation Systems Center, Tech. Rep. Final Report, Aug. 2001.

[7] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, and P. Kintner Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GNSS'08, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.

[8] UT Austin Researchers Successfully Spoof an 80 Million Dollar Yacht at Sea (2013, July) [Online]. Available: https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

[9] J. Bhatti and T. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," The University of Texas at Austin, Tech. Rep., 2014.

[10] M. Russon. (2015, May) Wondering how to hack a military drone? It's all on Google. International Business Times. [Online]. Available: http://www.ibtimes.co.uk/wondering-how-hackmilitary-drone-its-all-google-1500326

[11] T. Humphreys, "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing," The University of Texas at Austin, Tech. Rep., Jul. 2012, submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security

[12] C. Sebastian. (2016, Dec.) Getting lost near the Kremlin? Russia could be 'GPS spoofing'. [Online]. Available: https://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/

[13] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," Journal of Field Robotics, vol. 31, no. 4, pp. 617–636, Jul. 2014.

[14] M. Psiaki and T. Humphreys, "GNSS Spoofing and Detection," Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, Apr. 2016.

[15] M. Kuhn, "An asymmetric security mechanism for navigation signals," in Proc. 6th Int. Conf. IH, Toronto, ON, Canada, 2004, pp. 239–252.

[16] P. Papadimitratos and A. Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures," in IEEE Military Communications Conference, MILCOM'08. San Diego, CA, USA: IEEE, Nov. 2008, pp. 1–7.

[17] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in Proc. 16th Int. Tech. Meet. Satell. Div. ION GPS/GNSS, Portland, OR, USA, Sep. 2003, pp. 1543–1552.

[18] O. Pozzobon "Keeping the spoofs out, signal authentication services for future GNSS." Inside GNSS, 6, 3 (May/June 2011), 48—55.

[19] "Authenticating GNSS: Proofs against spoofs, Part 2," Inside GNSS, pp. 71–78, September/October 2007.

[20] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal Authentication, A Secure Civil GNSS for Today," Inside GNSS, Vol. 4, No. 5, Sept./Oct. 2009, pp. 30-39.

[21] B. O'Hanlon, et al. "Real-time spoofing detection in a narrow-band civil GPS receiver." Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2010), Portland, OR, Sept. 21—24, 2010, pp. 2211—2220.

[22] L. Heng, D. Work, and G. Gao "GPS Signal Authentication from Cooperative Peers" in IEEE Transactions on Intelligent Transportation Systems, Vol. 16, No. 4, August 2015

[23] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals" in IEEE Transactions on Aerospace and Electronic Systems Vol. 49, No. 4, October 2013

[24] A. Ranganathan, H. Olafsdottir, and S. Capkun, "SPREE: A Spoofing Resistant GPS Receiver," in ACM Conference on Mobile Computing and Networking, MobiCom'16. New York, USA: ACM, Oct. 2016, pp. 348–360.

[25] N. Tippenhauer, C. Popper, K. Rasmussen, and S. Capkun, "On the Requirements for Successful GPS Spoofing Attacks," in ACM Conference on Computer and Communications Security, CCS'11. Chicago, IL, USA: ACM, Oct. 2011, pp. 75–86.

[26] K. Jansen, N. Tippenhauer, and C. Popper, "Multi-Receiver GPS ¨ Spoofing Detection: Error Models and Realization," in Annual Computer Security Applications Conference, ACSAC'16. Los Angeles, CA, USA: ACM, Dec. 2016, pp. 237–250.

[27] P. Montgomery, T. Humphreys, and B. Ledvina, "ReceiverAutonomous Spoofing Detection: Experimental Results of a MultiAntenna Receiver Defense Against a Portable Civil GPS Spoofer," in International Technical Meeting of The Institute of Navigation, ION'09, Anaheim, CA, USA, Jan. 2009, pp. 124–130.

[28] P. Swaszek and R. Hartnett, "Spoof Detection Using Multiple COTS Receivers in Safety Critical Applications," in International Technical Meeting of The Satellite Division of the Institute of Navigation, ION GNSS+'13, Nashville, TN, USA, Sep. 2013, pp. 2921–2930.

[29] P. Swaszek, R. Hartnett, M. Kempe, and G. Johnson, "Analysis of a Simple, Multi-Receiver GPS Spoof Detector," in International Technical Meeting of The Institute of Navigation, ION'13, San Diego, CA, USA, Jan. 2013, pp. 884–892.

[30] M. Psiaki, B. O'Hanlon, S. Powell, J. Bhatti, K. Wesson, T. Humphreys, and A. Schofield, "GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase," in International Technical Meeting of The Satellite Division of the Institute of Navigation, ION GNSS+'14, Tampa, FL, USA, Sep. 2014, pp. 2776–2800.

[31] K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt, "Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks," in IEEE Symposium on Security and Privacy (SP), 2018

[32] G. Liu, R. Zhang, C. Wang, and L. Liu, "Synchronization-Free GPS Spoofing Detection with Crowdsourced Air Traffic Control Data," in 20th IEEE International Conference on Mobile Data Management (MDM), 2019

[33] D. Yu, A. Ranganathan, T. Locher, S. Capkun, and D. Basin, "Short Paper: Detection of GPS Spoofing Attacks in Power Grids," in ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec'14. Oxford, United Kingdom: ACM, Jul. 2014, pp. 99–104.

[34] OpenSky Network. (2017) OpenSky Network. [Online]. Available: https://opensky-network.org

[35] J. Tsui *Fundamentals of Global Positioning System Receivers: A Software Approach* 2000

[36] L. Shi, K. Sung, "Spectrum requirement for vehicle-to-vehicle communication for traffic safety" 79th Vehicular Technology Conference (VTC Spring), IEEE (2014), pp. 1-5

[37] W. Franz and H. Hartenstein, "Inter-Vehicle Communications, FleetNet project." University Karlruhe, 2005

[38] OSQZSS. (2017) Software-Defined GPS Signal Simulator. [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[39] u-blox, "u-blox M8 concurrent GNSS timing modules," 2016. [Online]. Available: https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf. [Accessed 20 11 2018].

[40] N. Store, "NS-RAW : CARRIER PHASE RAW MEASUREMENT OUTPUT GPS RECEIVER," SkyTraq, [Online]. Available: http://navspark.mybigcommerce.com/ns-raw-carrier-phase-raw-measurement-output-gps-receiver/. [Accessed 21 11 2018].

[41] F. Fasching, "RasPiGNSS Aldebaran," Franz Fasching Information-Telecommunications-Technology, [Online]. Available: https://drfasching.com/products/gnss/raspignss.html. [Accessed 21 11 2018].

[42] S. Navigation, "Piksi Multi GNSS Module," Swift Navigation, [Online]. Available: https://www.swiftnav.com/store/gnss-sensor-volume-orders/piksi-multi-gnss-module?[Accessed 21 11 2018].

[43] C. Bettisworth, M. Burt, A. Chachich., R. Harrington, J. Hassol, A. Kim, and G. Ritter, "Status of the dedicated short-range communications technology and applications: report to Congress (No. FHWA-JPO-15-218)." United States. Department of Transportation. Intelligent Transportation Systems Joint Program Office. Available at https://www.its.dot.gov/research_archives/connected_vehicle/pdf /DSRCReportCongress_FINAL_23NOV2015.pdf].