Digital Radio Signal Cancellation Attacks

An Experimental Evaluation

Daniel Moser[*]
armasuisse Science + Technology
Thun, Switzerland
daniel.moser@armasuisse.ch

Vincent Lenders
armasuisse Science + Technology
Thun, Switzerland
vincent.lenders@armasuisse.ch

Srdjan Capkun
ETH Zürich
Switzerland
srdjan.capkun@inf.ethz.ch

ABSTRACT

Attacker models are the cornerstone of any security assessment. As attacker's capabilities evolve over time, it is key to re-evaluate periodically if attacker models that were deemed unrealistic in the past might not pose a possible threat today. In this work, we evaluate the threat of wireless radio signal cancellation attacks in the face of recent advancements in software-defined radio attacker capabilities. Unlike classical radio interference or jamming attacker models which add noise to the legitimate communication, signal cancellation attacks aim at interfering destructively with the legitimate signal in order to remove those signals from the spectrum. While signal cancellation attacks were deemed unrealistic in the analogue domain, we analyse the system requirements to perform such attacks digitally using SDRs and evaluate the feasibility to launch such attacks against wireless communication systems such as GPS. Our evaluation reveals that signal cancellation attacks that manage to attenuate up to 40 dB of the signal at the receiver are feasible over the air. We further show that even complex CDMA signals such as GPS can be attenuated by 30 dB, even below a receiver's noise floor. These results indicate that digital signal cancellation attacks – especially against systems like GPS – should not be considered impossible per se, but deserve consideration when assessing the threat of attacks on wireless communication systems.

ACM Reference Format:
Daniel Moser, Vincent Lenders, and Srdjan Capkun. 2019. Digital Radio Signal Cancellation Attacks: An Experimental Evaluation. In *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3317549.3319720

1 INTRODUCTION

Radio jamming is an effective way to disrupt wireless communications. By radiating interference on the same frequencies as legitimate transmissions, jammers are able to prevent neighbouring receivers from correctly decoding the legitimate signals and thus block communication. Jamming originates from the military domain, however, deliberate jamming attacks are also commonly encountered in non-military contexts as well. For example, jamming devices targeting cellular networks [16, 27], wireless sensor networks [26], satellite navigation signals [12], wireless LANs [24], or IMDs [11] have been well investigated in the literature.

When a jamming signal interferes with the signal of a legitimate transmitter, the resulting signal at the receiver is the superposition of both signals. A common jamming approach sends a signal that resembles noise, such as random Gaussian noise directly mixed with the carrier, or an arbitrary signal modulated onto a carrier. Irrespective of the form of interference, the common assumption is that the jamming signal adds up *constructively* to the legitimate signal, therefore increasing the noise level at the receiver. This has the effect of reducing the signal-to-noise ratio (SNR) or even overshadowing the legitimate transmission.

An alternative form of interference that is not usually considered in wireless networks is destructive interference. When a jammer sends a signal that is an inverted version of the legitimate signal, both signals could interfere *destructively* and the legitimate signal at the receiver is annihilated. Destructive interference is a well-known phenomenon in physics and science fiction, as famous science fiction author Philip K. Dick wrote in his book *Do Androids Dream of Electric Sheep?* [6] from 1968:

> Setting down his weapons kit he fumbled it open, got out a nondirectional Penfield wave transmitter; he punched the key for catalepsy, himself protected against the mood emanation by means of a counter-wave broadcast through the transmitter's metal hull directed to him alone.

Signal cancellation attacks are in principle as effective as classical jamming attacks since they decrease the SNR at receivers. However, they are rarely considered in the wireless network security literature. The main reason is that destructive interference is more challenging to achieve because the attacker has to match the target signal with an inverted version that arrives at the receiver with very accurate timing, phase, carrier frequency, and amplitude synchronisation. The common assumption is that radio signal cancellation attacks are too difficult to succeed in practice [19, 23] and existing anti-jamming techniques thus ignore such threat models [3, 25].

In this paper, we revisit this assumption and analyse the specific requirements necessary to perform signal cancellation attacks. In particular, we develop an attacker model leveraging the fact that certain digital signals are predictable as a whole or in parts. For example, satellite-based navigation signals such as GPS can be determined in advance, knowing the locations of the satellites and the time.

Given the predictable nature of GPS signals, we show that it is possible for an attacker to create matched signals that attenuate

[*] Also with ETH Zürich.

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05.
https://doi.org/10.1145/3317549.3319720

the received signal strength remotely over the air by up to 40 dB irrespective of the relative location of the attacker to the receiver. Depending on the SNR at the receiver, this level of attenuation can be sufficient to make signals completely disappear from the spectrum, i.e., to attenuate the signal below the noise floor of the receiver. Thus, our results indicate that the signal cancellation attacker should not be ignored prematurely in anti-jamming works.

The rest of this paper is arranged as follows. In Section 2 we introduce the contributions of our work, followed by the background Section 3. We investigate a previous signal cancellation attacker in Section 4 and introduce our own attacker model in Section 5. We evaluate the feasibility of such attacks in Sections 6 through 8. We then discuss how the attacker could learn the signal properties in Section 9. This paper is concluded with related work and conclusions in Sections 10 and 11.

2 CONTRIBUTIONS

While signal cancellation attacks were described conceptually in the literature [4, 10, 17, 19], there is little work on the actual feasibility of such attacks. The effects and success factors of cancellation attacks are therefore not well understood and are almost never considered as a threat model in the development of anti-jamming communication techniques. To our knowledge, this work is the first to systematically investigate such attacks and to demonstrate the feasibility of successful cancellation attacks over the air on complex signals such as GPS in a laboratory environment. Our work provides an assessment of the feasibility and impact of signal cancellation attacker models.

The main contributions of this work are as follows:

- We first evaluate the accuracy requirements towards signal alignment of amplitude, frequency, and phase in order for a signal cancellation attack to be successful.
- We evaluate how signal imperfections and attack geometry impact the ability of performing signal cancellation in the analogue domain.
- We demonstrate the feasibility of digitally cancelling an unmodulated carrier signal for different signal strengths and transmission mediums in the lab. Our results show that digital signal cancellation attacks can attenuate the signal by more than 30 dB over distances of up to 25 m irrespective of the attackers position.
- We demonstrate the feasibility of cancelling GPS signals which have a complex modulation. We show that it is possible to attenuate the entire GPS signal by 30 dB under the receiver's noise floor. Furthermore, we show that it is possible to completely cancel the signals from individual satellites without affecting the signals from other satellites. This is particularly powerful since a number of GPS anti-spoofing techniques assume the presence of legitimate signals.
- We evaluate the accuracy of a GPS carrier phase estimation technique to estimate the phase offset that an attacker needs to minimise in order to be successful.

3 DESTRUCTIVE INTERFERENCE PRIMER

Destructive interference, also known as *signal cancellation* or *nulling*, describes the result of a special interference pattern, where two

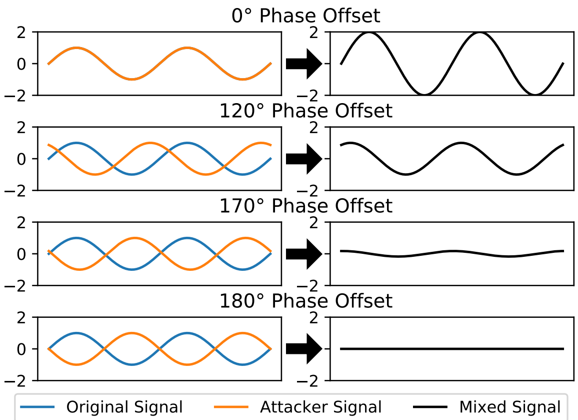

Figure 1: Effect of a signal overlaid with a copy of itself with different phase offsets.

signals overlap and as a result cancel each other out. More formally, we introduce a signal from a jammer $s_J(t)$ that interferes with a signal from a transmitter $s_T(t)$. The resulting signal at a receiver $s_R(t)$ is the superposition of both signals plus the noise $n(t)$:

$$s_R(t) = s_T(t) + s_J(t) + n(t) \tag{1}$$

For illustration purposes, we consider two unmodulated carrier signals for $s_T(t)$ and $s_J(t)$. Let f be the frequency, A the amplitude, and ϕ the phase, we can then write the signals as follows:

$$\begin{aligned} s_T(t) &= A_T \cdot \sin(2\pi f_T \cdot t + \phi_T) \\ s_J(t) &= A_J \cdot \sin\left(2\pi f_J \cdot t + \phi_J\right) \end{aligned} \tag{2}$$

Perfect destructive interference occurs when the amplitude and frequency of both signals are identical, the noise is zero, and the phase has an offset of half a wavelength

$$A_T = A_J \wedge f_T = f_J \wedge \phi_T = \phi_J \pm \pi \wedge n(t) = 0, \tag{3}$$

or if the frequency and phase are aligned but the amplitudes of both signals have opposite signs

$$A_T = -A_J \wedge f_T = f_J \wedge \phi_T = \phi_J \wedge n(t) = 0. \tag{4}$$

In reality, it may not be possible to achieve perfect alignment and zero noise. Thus, it is more practical to introduce the attenuation factor D as a metric to quantify the level of destructive interference. The attenuation can be understood as the ratio between the amount of signal power from the transmitter and the total power from the superimposed signals. In decibels, D can be represented as:

$$D = 10 \cdot \log_{10} \left(\frac{s_T(t)}{s_T(t) + s_J(t) + n(t)} \right)^2 \tag{5}$$

Already small misalignments in amplitude, frequency and phase could potentially lead to only weak signal attenuation or even to signal amplification, i. e., constructive interference with a negative D. Figure 1 displays the effect of signal misalignment for the example of phase offsets. A phase offset of *zero* will amplify the original signal to double its amplitude ($D = -6\,dB$) and a phase offsets of 120 degrees does not attenuate the signal at all ($D = 0\,dB$). A phase offset of 170 degrees manages to significantly attenuate the resulting signal ($D > 0\,dB$), while a phase offset of exactly π is required to entirely attenuate the resulting signal to zero ($D \gg 0\,dB$).

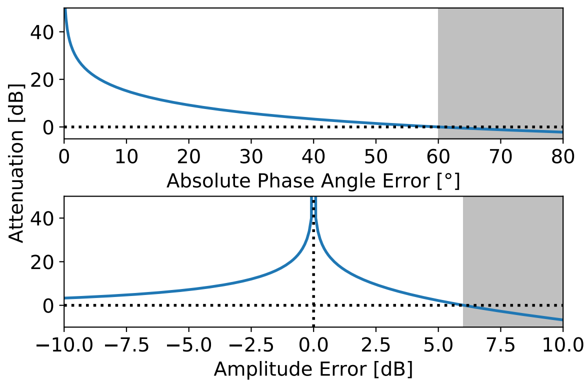

Figure 2: Influence of phase (top) and amplitude (bottom) error on achieved attenuation.

To quantify the requirements for successful signal cancellation attacks, we simulated the effect of the jammer deviating from its desired amplitude, phase and frequency on the resulting attenuation at the receiver. For each simulation, we assumed that only one parameter (A_J, f_J, or ϕ_J) deviates from the desired value according to Equations (3) and (4).

Figure 2 shows the effect of the attacker deviating from its desired 180° phase offset. At an error of 60° the attacker already stops attenuating the signal and with every degree of phase error added will amplify the legitimate signal at the victim's antenna. On the other hand, the attacker's signal's amplitude will only start amplifying the legitimate signal after an error of 100%. An amplitude error of less than 20% amounts to an attenuation of more than 10 dB.

The frequency error, contrary to the amplitude and phase errors, does not introduce a static attenuation. The frequency error generally depends on the accuracy of the local oscillator of a transmitter, which is usually specified in parts per million (ppm). When two waves with a small frequency offset overlap, a physical effect called beat is created. The resulting signal will itself be a new wave with a frequency of $f_B = |f_T - f_J|$. The effect of this beat on signal amplitude over time is shown in Figure 3. This simulation assumes an unmodulated carrier signal with a frequency of 1 GHz. The results of this simulation show that the longer the signal the attacker wants to cancel, the lower the clock error of its device needs to be. With modern commercial off-the-shelf SDR hardware, we can expect errors around 10 ppm. In the upper segment of lower cost hardware, we can find devices that are equipped with GPS disciplined oscillators. Such a device would be the USRP X300 by Ettus, which offers a frequency accuracy of 10 ppt when locked to GPS [7].

4 THE ANALOGUE SIGNAL CANCELLATION ATTACKER

After this discussion on the requirements of a successful signal cancellation attacker, we are now going to discuss the limitations of an analogue signal cancellation attacker. To the best of our knowledge, the only practical demonstration of a signal cancellation attack was reported by Pöpper et al. [17]. A straightforward implementation is using two antennas and a delay-line or phase shifter which outputs the signal at the second antenna in such a way that the

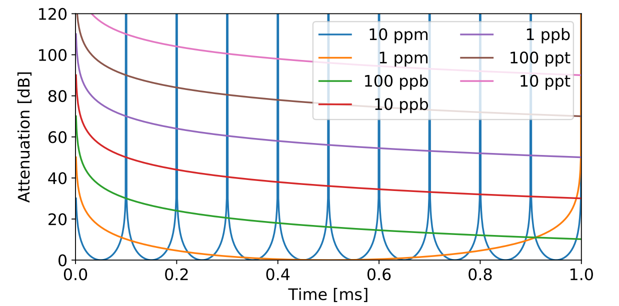

Figure 3: Effect of frequency errors on achieved attenuation.

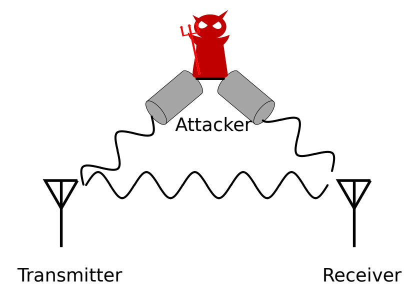

Figure 4: Attacker model for the analogue signal cancellation attacker. Note that the attacker would need an antenna array for broadband signals, arranged in a way for all frequencies present in the transmission being properly phase-shifted and therefore cancelled at the receiver.

legitimate and the attacker's signals arrive at the victim's receiver phase shifted by half a carrier wave length (see Figure 4). The results have shown the ability to attenuate a legitimate transmission in a laboratory environment by 23 dB over a distance of less than 2 m [17].

The main limitation for the attacker is its positioning. Because it directly relies on receiving and forwarding the legitimate transmission, the attacker is highly confined in space. In such a system, we have the distance between transmitter and receiver (d_{tr}), transmitter and attacker (d_{ta}) and attacker and receiver (d_{ar}). The time delay between legitimate and attacker signals can be expressed as

$$\Delta t = \frac{d_{ta} + d_{ar} - d_{tr}}{c}. \tag{6}$$

Additionally, we can calculate the duration of a symbol by $t_{Symbol} = 1/f_{Symbol}$, where f_{Symbol} is the symbol rate.

Assuming the attacker achieves perfect carrier phase alignment with π offset at the receiver, the signals are still delayed by the additional path travelled Δt. Figure 5 shows the effect of different offsets on the legitimate signal. Even an offset of 0.1 symbols will leave short – but strong – peaks in the spectrum that can be detected by the legitimate receiver. Thus, the attacker's goal is to minimise symbol delay as much as possible, yielding

$$\Delta t \ll t_{Symbol} \tag{7}$$

as the main requirement for the attacker's positioning in the system.

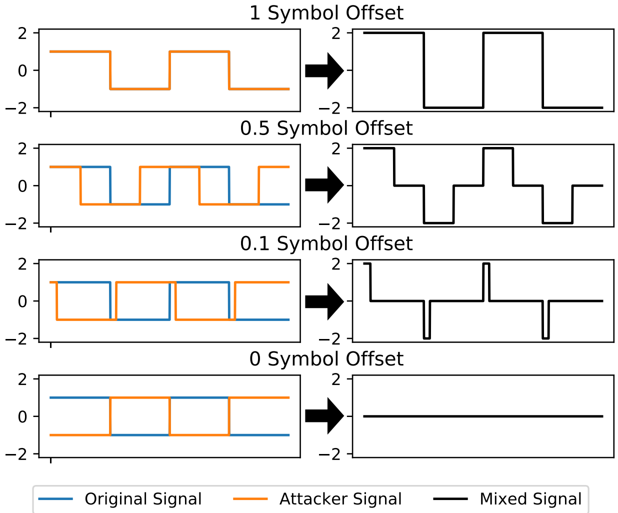

Figure 5: Effect of different symbol delays on a BPSK baseband signal under the assumption that the carrier phase of the attacker's signal is perfectly shifted by a factor of π.

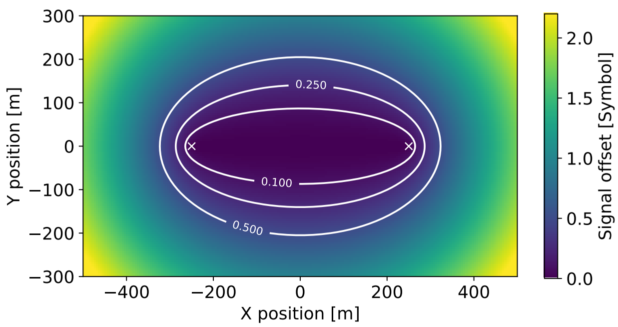

Figure 6: Symbol delay for an analogue signal cancellation attacker attacking a signal sent by the legitimate transmitter on the left and received by the legitimate receiver on the right over a distance of 500 meters. The contour lines describe the area within which the delay is smaller than half, a quarter and a tenth of a symbol duration.

In other words, it is confined to an elliptic space, defined by the maximum amount of symbol delay the attacker is willing to accept. In Figure 6 we simulated a 1MHz BPSK signal over an area of 1 km^2 with the legitimate transmitter and receiver positioned 500 meters apart on the center axis. The contour lines depict the maximum distance the attacker can position itself without having more than the specific symbol offset. Higher data rates will force the attacker more and more towards the direct path between transmitter and receiver.

In addition, the attacker has to receive the legitimate signal, delay or phase shift it by half a carrier cycle and retransmit the shifted signal over a second antenna. Within the attacker's system, the signal will encounter small time delays between entering the receive antenna and exiting through the antenna towards the victim, which will again force the attacker closer to the direct transmission path between transmitter and receiver.

This analogue attacker model is therefore considered limited because it strongly couples the attacker to the legitimate signals. The attacker needs to position itself very close to the direct transmission path in order to achieve the required timing synchronisation.In many real-world scenarios, these space constraints therefore severely limit the threat of this attacker model.

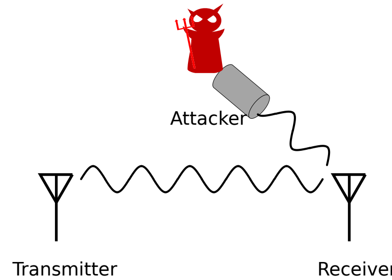

Figure 7: Model of the digital signal cancellation attacker.

5 THE DIGITAL SIGNAL CANCELLATION ATTACKER

In this section we introduce the *digital* signal cancellation attacker, which is not constrained in space. Our system model includes, as previously, a legitimate transmitter and an attacker both equipped with either an omnidirectional or directional antenna. The legitimate receiver is equipped with an omnidirectional antenna. None of the legitimate players make use of multiple antenna or any other Multiple Input Multiple Output (MiMo) schemes. While the attacker could be equipped with additional antennae and receivers, they do not directly play part in the signal cancellation but only give additional information on the legitimate signal.

The legitimate transmitter sends a signal, modulated onto a carrier, which – in turn – the legitimate receiver receives. Our work makes no assumption or requirement on the modulation scheme but we assume that the attacker can predict some parts or the whole signal from the legitimate transmitter. Predictable signals are encountered in many wireless communication systems. For example in GPS, the signal is entirely determined by the position of the satellites – also called space vehicle (SV) – and the time which are all deterministic values. In LTE, fixed pilot signals are used to help the mobile nodes synchronise to the base stations. WiFi signals exhibit constant preambles or packet headers which are sent repetitively. In wireless sensor networks, slowly and rarely changing values such as temperature measurements will lead to several identical packet transmissions.

The digital signal cancellation attacker exploits predictable parts of the signal to create locally a digital copy of the signal to be cancelled. The attacker then transmits this copy independently from the transmitter's signal such that it collides at the receiver with the one of the transmitter with a phase offset of π. As in the analogue signal cancellation model, the digital attacker needs to accurately estimate the victim's antenna position and phase, but the digital attacker model is not constrained geographically which makes it possible to launch such cancellation attacks from any

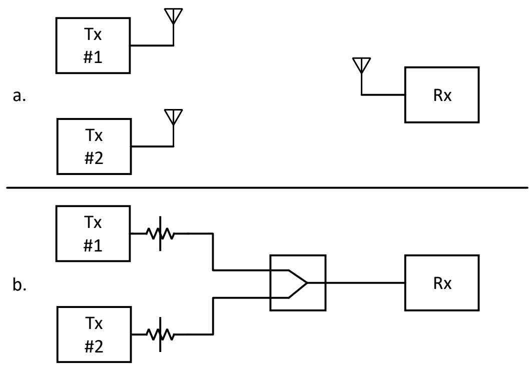

Figure 8: Overview over our laboratory setup. We use two transmitters equipped with directional antennae and a receiver with an omnidirectional antenna (a.). For more controlled channel conditions, we use a cable-based setup, where the two transmitters are connected to attenuators, then the signal is mixed using a signal combiner before entering the receivers' radio front-end (b.).

position relative to the transmitter and receiver. The challenge lies in creating a digital copy of the signal that is as close as possible to the transmitter's signal without the ability to observe the signal waveform from the air as in the case of the previously described analogue signal cancellation model.

The rest of this paper represents a feasibility study of the digital attacker. We evaluate current hardware constraints under laboratory conditions to quantify the impact of such attacks.

6 EXPERIMENTAL SETUP

In our evaluations of the possible attenuation of such attacks, we make use of the following devices. On the transmitter side, we use two USRP X300 manufactured by Ettus and equipped with SBX400 daughterboards. The transmitters are synchronised through an external clock signal. On the receiver side, we use an FSQ8 signal analyser by Rhode & Schwarz for direct signal strength and spectrum measurements. For non-spectrum GPS measurements we use a commercially available u-blox M8 GNSS Evaluation Kit EVK-M8T.

We use two different setups to evaluate the signal cancellation. In one setup (Figure 8a) we attach antennae to both transmitters and receiver and use the air as transmission medium. In the second setup (Figure 8b), we connect the transmitters and receiver with coaxial cable, mixing the two signals with a signal combiner and feeding them into the receiver. A cable-based setup helps us remove any interference of the indoor, multipath-rich channel in the lab. If not stated differently, each used cable was of a length of 60 cm and the antennas were placed on an equilateral triangle of side length 2 m.

To adjust the phase and amplitude of the attacker's signals we rely on GNURadio software which varies the values of the generated IQ samples. As GPS synchronisation of our transmitters is not possible within a shielded laboratory environment, we use a local clock to drive the local oscillators of the transmitters. We either use a single device with two transmission front-end – denoted *one stage synchronisation* – or two individual devices whose local oscillators are synchronised using an external clock – denoted *two stage synchronisation.*

To avoid legal problems, we transmit GPS signals over the air only in a shielded laboratory environment.

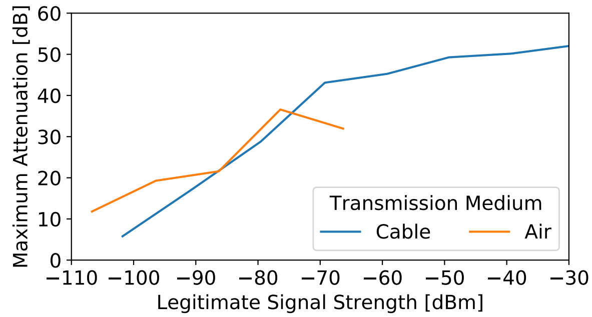

Figure 9: Achieved attenuation on an unmodulated carrier transmitted over coaxial cables and over the air. The attenuation over the cable flattens at approximately -70 dBm as both transmitters introduced additional noise into the spectrum.

7 DIGITAL SIGNAL CANCELLATION OF AN UNMODULATED CARRIER

We first evaluate the digital signal cancellation on an unmodulated carrier signal. The experiments shown were conducted both over coaxial cables and over the air. We transmit the carrier signal at a frequency of 1.5 GHz with 0 dB front-end gain to avoid additional distortions of the generated signal.

7.1 Attenuation vs. Transmission Power

At the transmitter, we generate different signal strengths in baseband, before transmitting, by varying the amplitudes from 0 $dBFS$ down in 10 dB steps.

Figure 9 depicts the achieved maximum attenuation for the cable and air setups. Due to higher path loss, the signal received over the air exhibits less dynamic range than the signal sent over the cable. The attenuation curve for the cable-based experiment flattens for signal strengths over -70 dBm. This effect is due to the transmitters, both the legitimate and the attacker's device, introducing distortions around the carrier and raising the noise floor. These distortions grew stronger with the signal's amplitude which explains why the attenuation curve is not linear. Such an effect is likely to happen for any radio transmitter, which means that high power transmissions are generally more difficult to attenuate than low-power signals.

In this experiment, we achieved a remarkable maximum attenuation of about 50 and 40 dB over coaxial cable and over the air, respectively. Note that these results do not indicate generally less attenuation over the air, as the signal levels for the transmissions over the air exhibited higher path loss.

7.2 Attenuation vs. Distance

In the next experiment, Tx#1 and Tx#2 are positioned approximately 5 meters apart. The receiver (Rx) is positioned in various distances

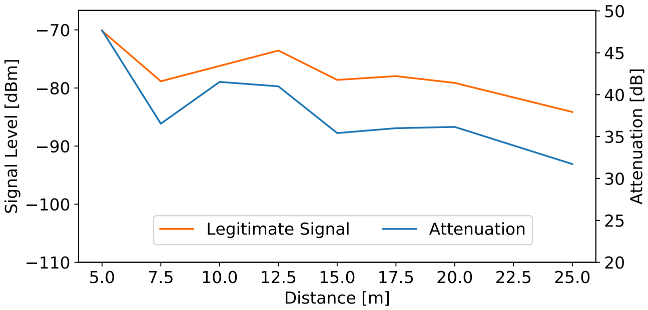

Figure 10: Achieved attenuation on an unmodulated carrier transmitted over the air over various distances, compared to the signal level without attack.

spaced in 2.5 m steps away from both transmitters and measured the peak signal power without the attacker's signal present. After the cancellation signal was activated, we measured the achieved attenuation for each distance. Figure 10 depicts the results. The achievable attenuation lowers slightly over the distance. However, this does not imply that the attack works worse over distance. The signal power without attack also shows a downwards trend due to path loss. Even over a distance of 25 m, the digital attacker cancels the legitimate signal by approximately 30 dB down into the noise floor. To our knowledge, these experiments are the first to demonstrate that signal cancellation attacks over more than 30 dB are possible over distances up to 25 m.

8 DIGITAL CANCELLATION OF GPS SIGNALS

In this section, we evaluate the feasibility of digitally cancelling GPS signals. GPS signals are quite complex given the CDMA modulation and the goal is to see if the same level of attenuation is possible as with the unmodulated carrier and if it is possible to cancel out individual satellite signal from the CDMA spectrum. Again, we evaluate this both through coaxial cables and over the air. We then evaluate how a commercial GPS receiver behaves in the signal processing chain when such an attack is conducted against individual satellites and the whole constellation. Finally, we evaluate the sensitivity towards the attacker's signals accuracy in both phase and amplitude.

To facilitate reproducibility, the GPS signals to be cancelled and the attacker's signals both are generated using the *gps-sdr-sim* software [15]. The attacker's digital signal is a phase-shifted copy in the baseband being transmitted over a second phase-coherent radio front-end. An important factor to consider is that GPS signals arriving on Earth's surface have a minimum guaranteed signal power of −128.5 dBm [21]. This signal strength is well below the noise floor of any receiver. GPS receivers use despreading techniques to raise the signal out of the noise. An attacker needs to attenuate its signals to a very low level, making the signal's properties more difficult to control.

8.1 Over the Noise Floor

To prove that we are indeed attenuating the legitimate GPS signal, we first show the attenuation above the noise floor, before moving to more realistic GPS power levels.

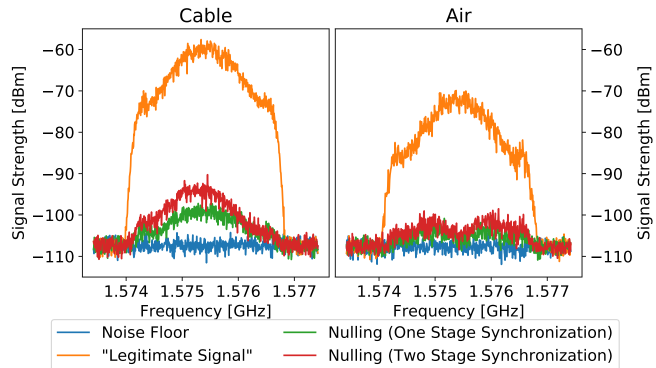

Figure 11: Power spectral density of the legitimate signal, the noise and cancellation attacks with different synchronisation methods.

We first evaluate the general receiver noise without any transmissions to know our baseline towards which to attenuate the transmitted signals. Second, we transmit the legitimate signal only, to calculate its signal power. Finally, we send both legitimate and attacker signals, to evaluate the achievable attenuations for an attacker. Table 1 gives an overview of these results while Figure 11 shows the power spectral density of said signals.

In the cable-based setup, the attacker is able to attenuate all frequencies present in the legitimate signal equally, i.e. the signal retains its shape at a lower level. Over the air in the indoor laboratory environment, some frequencies were subjected to higher cancellation (near the center frequency) while others were less attenuated (approximately 0.5 MHz from the center frequency). This can be explained due to the multi-path, indoor environment. When a signal containing multiple frequencies follows the same multipath, the phase offset of each frequency will alter slightly. The signals refracted off the walls take the same physical distance, however, due to the different wave lengths, the phase for each part of the individual frequencies will exhibit a different offset. Which leads to nearly perfect attenuation at the center frequency but less optimal attenuation in the flanks of the GPS spectrum as seen in Figure 11. The attacker's signal will therefore not interfere destructively with each frequency in the most desirable way for the attacker.

In this experiment, Table 1 shows how we achieved an average attenuation over the GPS spectrum of 37.4 dB and 33.5 dB for one and two stage synchronisation over cable. Over the air, the average attenuation was 28.2 dB and 26.5 dB due to the higher path loss of the legitimate signal and multi-path interfering with the attacker's signals and therefore not attenuating each frequency by the same amount.

8.2 Below the Noise Floor

We now evaluate if the attenuation we achieved previously is also effective enough at more realistic GPS signal powers, i.e. at around 25 $dBHz$ and 35 $dBHz$ after the GPS receiver's despreading processing gain.

We connect the two transmission front-ends to the radio input of our commercial GPS receiver and insert attenuators into the signal path to bring the GPS signal to a realistic power level of 28 $dBHz$ at the receiver after the processing gain. Figure 12 shows

Signal	Cable Average Power [dBm]	Cable Peak Power [dBm]	Air Average Power [dBm]	Air Peak Power [dBm]
None	-107.23	-104.24	-107.54	-104.24
Legitimate	-63.97	-57.59	-76.53	-69.91
Nulling (One Stage)	-101.36	-97.21	-104.77	-100.82
Nulling (Two Stage)	-97.48	-90.26	-102.99	-98.50

Table 1: Signal powers for our three scenarios, evaluating the maximum achievable attenuation for the attacker.

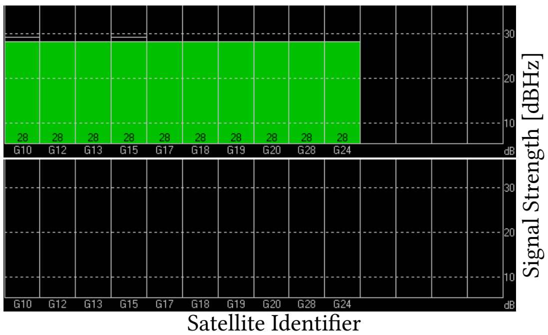

Figure 12: Signal strengths per satellite as reported by our GPS receiver, before (top) and after (bottom) launching the signal cancellation attack.

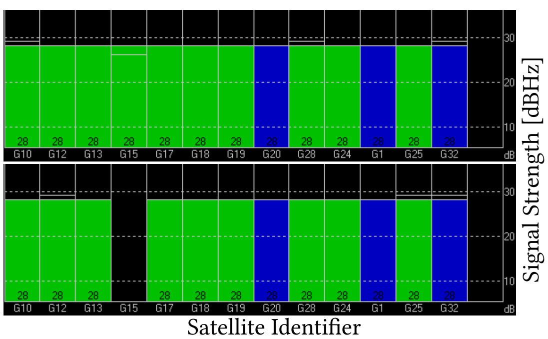

Figure 13: Signal cancellation attack on an individual satellite's signals.

the receiver's signal strength for each satellite with and without the signal cancellation attack. All satellite's signals were cancelled while the attack is on.

These results confirm that it is possible to cancel the GPS signals below the noise floor of the commercial GPS receiver, making the digital signal cancellation attack stealthy.

8.3 Selective Cancellation of Individual Satellites

GPS applies code spreading (CDMA) to separate the individual satellite's signals from the superimposed signal in the receiver's signal processing chain. It should then be possible to attenuate the signal from an individual satellite without interfering with the rest of the constellation. To test this assumption, we generated a

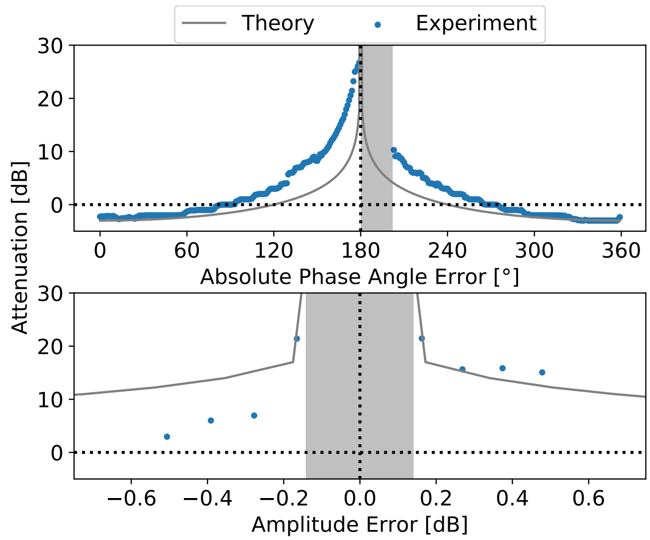

Figure 14: Average signal strength reported by our GPS receiver over all satellites in relation to the phase and amplitude of the attacker's signal. Grey areas denote loss of signal for the receiver.

secondary GPS signal for the same time frame, containing a single satellite's signal. Instead of sending the superimposed signal over the attacker's front-end, we now only send this individual signal. Figure 13 confirms our assumption, showing the signal strength per satellite before (top) and during the attack (bottom). An attacker can thus impact individual transmissions on a shared medium at will without disrupting other transmissions, drastically reducing the chance of detection.

This technique of individually cancelling satellite's signals can be used to stealthily take over the victim's positioning. The attacker could replace each satellite's signal with a spoofed version, therefore also potentially not alerting the victim because it should not lose position lock when attacked in such a way.

8.4 Effects of Systematic Phase and Amplitude Errors

As shown in Section 3, the attacker's signals need to be within a certain window with regards to phase and amplitude offsets. We evaluated how near to the optimal phase and amplitude the attacker needs to be tuned in order to have a significant impact on the transmitted signal without distorting it. Figure 14 shows the average signal strength over all satellites as reported by our GPS receiver in relation to the attacker's signal phase (top) and amplitude (bottom). It shows that the attacker is initially required high accuracy in both amplitude and phase of its signals. After the initial successful cancellation, however, we see that the commercial GPS receiver needs a certain signal strength in order to recover the satellite signals again. As we iterated through all phase-shifts for each amplitude, we can see that the receiver only locks to the satellites' signals again when reaching around $20dBHz$ of signal strength. The measured attenuation was higher than theory suggests in the case of phase-only error. We assume this mismatch to occur by how the commercial receiver processes the signal and calculates the power of the despread signal. For the amplitude error, the attacker achieved less attenuation than expected. This was due to the fact that the transmitter lost individual digital samples, which resulted in a phase shift of the signal in the analogue domain.

The results of this experiment confirm our simulations in Section 3. Further, it shows that tens of degrees of phase error still allows the attacker to attenuate the whole GPS constellation by approximately $10\,dB$ and by $20\,dB$ for errors of approximately 5°.

9 PARAMETER ESTIMATION FOR A REMOTE RECEIVER

In this section, we evaluate the challenges for any signal cancellation attacker – both *analogue* and *digital*. The attacker needs knowledge about the signal's amplitude and phase at the victim's antenna in order to properly cancel any signal. So far in our experiments, we estimated the phase and amplitude manually, but an attacker will not have local access to the receiver and needs to estimate those parameters automatically.

9.1 Signal Amplitude

The first parameter the attacker needs to find is the signal's amplitude at the remote receiver. As long as the terrain for both the attacker and victim are very similar due to the required proximity of the attacker, the attacker can assume GPS power levels at the victim to be very similar to its own measured signal power. The attacker does not need to know about the victim's antenna gain as long as the actual power of the GPS signal can be determined. This is owed to the fact that the attack happens in the air in front of the victim's antenna and the signal entering the antenna is already the superposition of the legitimate and the attacker's signals.

9.2 Carrier Phase

The second parameter crucial for launching successful signal cancellation attacks is the carrier phase of the legitimate signal. We introduce a possible approach how an attacker could determine and track the carrier phase offset between its antenna and the victim's antenna location.

9.2.1 Carrier Phase at the Attacker's Receiver. To determine the signal's phase at the remote receiver, the attacker can evaluate the signal's carrier measurements at its own position. As the GPS signal is a superposition of all visible space vehicle's signals, we estimate the phase development for individual SVs first. Adding the individual SV's carrier phase measured at the same time gives us the phase of the raw signal as it is received at the radio front-end.

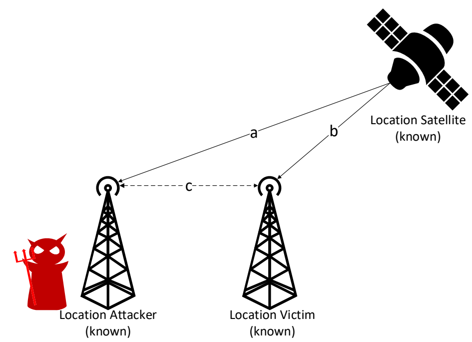

Figure 15: System geometry with the different signal paths.

In a system where a space vehicle and the GPS receiver stand still and the channel is not distorting the signal, the carrier wave can be modelled as

$$F(t) = \sin(2\pi \cdot f \cdot t + \phi_i), \tag{8}$$

where $f_c = 1.574\,GHz$ is the GPS carrier frequency and ϕ_i is the initial phase offset of the signal. We then determine the phase angle (ϕ_c) for any given moment t as

$$\phi_c(t) = 2\pi \cdot f \cdot t + \phi_i \pmod{2\pi}. \tag{9}$$

Extending this model to a more realistic scenario, we take into account the relative movement of the SV in relation to a GPS receiver. In general, the SV first approaches the receiver after rising above the horizon and will then transition to a state where it departs again. We thus take the Doppler shift into account, which due to the movement of Earth and the SV can be modelled as a sine wave with a very long wavelength. Due to the constantly changing frequency of the signal, we can no longer directly apply Equation 9 and account for the changing frequency at time t. If we do that, we would experience phase discontinuities as calculating the phase for a given frequency and a given time in Equation 9 would assume a wave that started at $t = 0$ with this frequency. We therefore sum the phases up for each step, as if they were very short individual waves between the sampling points:

$$\phi_c(t) = \sum_{n=0}^{t \cdot f_s} \left(2\pi \cdot (f_c + f_d(t)) \cdot \frac{1}{f_s} \right) + \phi_i \pmod{2\pi} \tag{10}$$

with f_s being the sampling frequency and $f_d(t)$ the Doppler shift frequency at time t.

9.2.2 Carrier Phase at the Victim's Receiver. We again begin with a static scenario from which we develop the dynamic solution. We assume the attacker knows its own position as well as the position of the victim very precisely. Additionally, through receiving the GPS signals, it receives the ephemeris data, from which it is able to calculate the precise position of each satellite at any given time during his attack. Figure 15 shows an overview over the system with one satellite and both receivers. As the positions of all three corners of the triangle are known, all three sides as well as all angles are known. We base our phase prediction scheme on a differential-GPS technique called Real Time Kinematic (RTK) [1]. In such a system, fixed basestations transmit their precise position, as well as the carrier-phase values for all received satellites to mobile nodes, which are then able to determine their position down to millimeter precision [8]. The node will calculate the difference of the carrier phases for pairs of satellites at the basestation and its own position to remove some atmospheric errors. We reverse the general idea of RTK through using the known position of all entities in this system and the carrier phase at the attacker's position to calculate the carrier phase at the victim's position. Because the baseline between attacker and victim is in the order of tens to hundreds of meters, we can base our calculations on each individual satellite. In a static setup the equation is

$$\phi_{victim} = \phi_{attacker} - \left(\frac{(a-b)}{\lambda} \cdot 2\pi\right) \pmod{2\pi}, \quad (11)$$

where $\phi_{attacker}$ is the carrier phase at the attacker's receiver, $(a-b)$ is the difference in the signal path between the satellite and the two receivers and $\lambda = 1/f$ is the wavelength of the GPS signal.

Combining Formulas 11 and 10, the attacker can now calculate the carrier phase at the remote receiver for each satellite. These values can then be tracked and used in the GPS signal generation to properly calculate the cancellation signal.

9.3 Evaluation of Location Errors on Carrier Phase Prediction

An unknown variable when conducting a signal cancellation attack is the precise position of the GPS satellite. While the satellites broadcast their ephemeris data that allow calculating the satellite's position at a variable time t, this ephemeris' error decreased with the lifetime of the GPS system due to advancements in measurement procedures. At the beginning of this millennium this error was around 2.6 meters [22] and has decreased to approximately 1.5 meters today [14]. An error of 1.5 meters translates to nearly eight phase cycles at the GPS carrier frequency. Additionally, the satellite moves approximately 300 meters between start of transmission and start of reception [20]. We have simulated the phase error for two receivers placed on earth's surface with a baseline of 20 meters and a satellite position offset of up to 1 kilometer in three dimensions around the calculated position. Within this radius, the maximum error is less than $0.03 rad$ due to the special geometry of the acute triangle between the two receivers and the satellites (see Figure 16).

The position error for the victim receiver, however, is much more severe on the phase prediction error. A position error of even 3 millimeters already translates to a theoretical phase prediction error of $0.1 rad$. Figure 16 depicts the minimum, maximum and mean phase error for victim misplacements of up to 10 centimeters.

Both simulations have shown that in the best case of a position error no phase error will occur. This special case happens if the geometry of the triangle *satellite-receiver-attacker* stays unchanged and only its orientation in space changes.

9.4 Validation of Carrier Phase Prediction

To validate our carrier phase prediction scheme, we deployed a USRP X300 with two antennas at distances of $20\,m$, which we measured using a laser range finder. Our recorded signals are post-processed using *gnss-sdr* [9]. We extracted the carrier phase measurements from the observables in addition to the broadcast

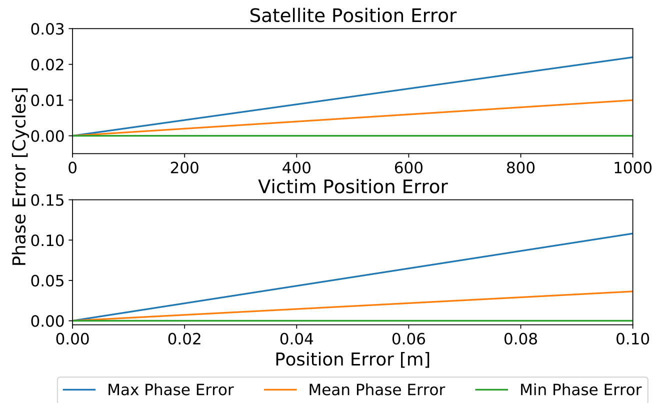

Figure 16: Impact of error of the satellite's position (top) and the victim's error (bottom) on the phase estimation for distances up to 1,000 (satellite) and 0.1 (victim) meters.

ephemeris provided by this software. Figure 17, shows the error between measured and predicted phase difference between the two antennae over the time of 20 minutes. It is apparent that not all satellites exhibit the same error, as would ideally be the case if we measured both our own and the victim's antenna position with high precision. We determined the locations of both antennas with the RTK method using an official reference station, approximately $15\,km$ away. The prediction for most satellites however stays nearly constant over the course of the experiment. Satellite 17's phase flips around one third into the experiment, which could be due to multipath at our experimental site close to a large metallic obstacle.

Assuming the attacker can detect and correct the initial phase offsets, we simulated how the phase error progressions influence the achievable attenuations of the individual space vehicle's signals during the attack. Figure 18 gives a visualisation of the attenuation over time. The phase jump by half a wave length of SV 17 results in these signals being amplified to double their signal strength. The attacker could theoretically achieve an attenuation of more than $20\,dB$ during the first minute. Afterwards certain SV's signal phase start to drift – especially satellites 9 and 22 – while the others are attenuated by more than $10\,dB$ during the whole measurement campaign.

Nevertheless, the results indicate our proposed phase prediction scheme works given that both antennas' location are precisely known. Satellites 3, 6 and 23 in particular exhibit a nearly constant phase prediction error and thus a very high theoretically achievable attenuation for the attacker.

10 RELATED WORK

Several publications deal with the detection of spoofers and jammers attacking the GPS system. SPREE [19] is a spoofing-detection GPS receiver that tracks multiple correlation peaks per satellite, if they occur, and evaluate if secondary peaks represent multipath or spoofed signals. Our work demonstrated an attacker that can remove the legitimate signal from the spectrum, thus removing the ability of SPREE to detect a signal spoofing attack. Recent work by Psiaki et al. [18] introduce different spoofing detection mechanisms

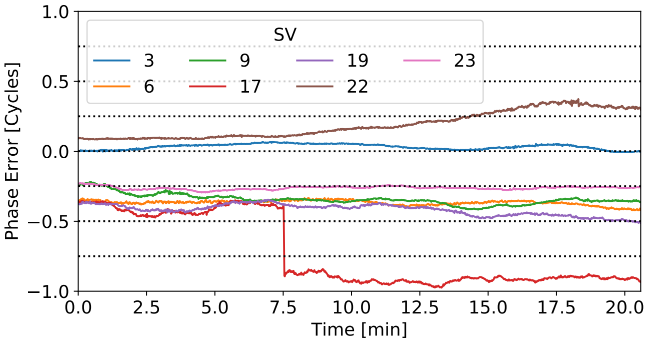

Figure 17: Calculated phase error over a distance of 20 meters tracked over a time of 20 min for all visible satellites.

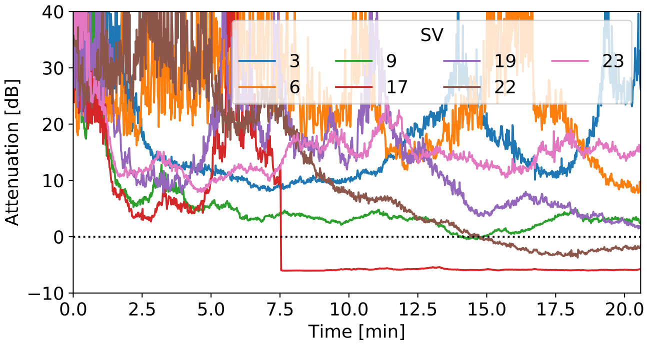

Figure 18: Theoretically achievable attenuation for the predicted phase progression with corrected initial values over a time of 20 min for all visible satellites.

but also discuss an attacker conducting a signal cancellation attack on the legitimate GPS signal. They mention that they conducted experiments on it but provide no empirical results. There is no information on the setup of the cancellation or if it occurs in the analogue or digital domain. We, on the other hand, take a detailed look at the requirements and the feasibility of such an attack. A detection approach based on power distortion measurements has been proposed by Wesson et al. [23]. Their approach detects both jamming and spoofing attacks reliably. However, they also explicitly exclude a signal cancellation attacker from their attacker model.

There exists previous work by DeBruhl et al. [5] describing a stealthy jamming attacker. The attacker itself is a classical jammer where the legitimate and jamming signals interfere constructively therefore introducing additional noise to the spectrum. The stealthiness of the attacker originates from the fact that it only transmits its signals periodically in short bursts, hence making detection and localisation of the jamming source much harder. Their approach introduces a trade-off evaluation by the attacker between how many packets it can jam and how little it transmits to avoid detection.

Signal cancellation has gained some traction in recent years [13, 18, 19]. One of the earlier publications by Pöpper et al. [17] evaluated the Dolev-Yao model where an attacker is able to flip bits of a transmitted message or annihilate the whole transmission. The limitations of their attacker is further described in Section 4. We, on the other hand, introduce an independent transmitter to transmit the cancellation signal. Clancy [4] presented a simulation on how efficient a nulling attack on an OFDM transmission's pilot would impact bit error rate. This differs, as we extensively evaluate a signal cancellation attacker's ability in both simulations and the real world. Bharadia et al. introduced a signal cancellation system to allow full duplex radios to operate with a single antenna [2]. Their system performs both analogue and baseband signal cancellation in order to remove the leaked transmitted signal from the received signal. Our proposed attack differs from this system in that we perform signal cancellation over the channel between a transmitter and a receiver. Additionally, we exploit the fact that certain signals are highly predictable in terms of content while Bharadia precisely know the signal transmitted by their own transmitter.

Interestingly, newer publications [10] take the signal cancellation attacker already as a given, building countermeasures without evaluating the actual threat. Their work introduces helper nodes that allows building a secure channel between a basestation and a new device requesting access to the basestation's network, without the attacker's node hijacking the connection.

11 CONCLUSIONS

In this paper, we have described and evaluated signal cancellation attacker models interfering with a legitimate signal on the physical layer. We have shown digital signal cancellation to attenuate a legitimate signal to a point where a receiver is not able to recover the information contained inside anymore. Such an attacker is even able to interfere with individual signals on a CDMA channel without affecting the other transmissions. We were able to attenuate simple carrier signals by up to 40 dB and more complex GPS signals by up to 30 dB over the air in a controlled set up. We have demonstrated such attacks for distances up 25 meters. These attenuation levels and distances are sufficient to bring many real-world signals below the noise floor of standard receivers and therefore make the signals disappear from the spectrum.

Our evaluation suggests such attacks could become more realistic than commonly assumed in the literature since the presented digital signal cancellation attacker model is not restricted to specific attacker's positions. Nevertheless our analysis has shown that certain challenges still remain in practice. First, the signal to be cancelled needs to be predictable. While many digital signals have at least some predictable parts, random or unpredictable signal parts cannot be cancelled with the presented digital attacker model. Second, the carrier phase of the attacker must be controlled very precisely and matched to the phase of the transmitter's signal at the receiver. We have investigated the ability of an attacker to determine the GPS carrier phase at a receiver. Our results indicate that the phase estimation using differential-GPS techniques is possible if the position of the receiver is known with high precision. This however, is a major challenge if the receiver is mobile. Nevertheless, a determined attacker could well achieve such a precision in fixed scenarios.

ACKNOWLEDGMENT

This work was partially supported by the Zurich Information Security and Privacy Center (ZISC). It represents the views of the authors.

REFERENCES

[1] J.P. Barboux. 1994. Practical Real Time Kinematic Applications of GPS. *Proceedings of DSNS 94, London, UK* (1994).

[2] Dinesh Bharadia, Emily McMilin, and Sachin Katti. 2013. Full Duplex Radios. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM (SIGCOMM '13)*. ACM, New York, NY, USA, 375–386. https://doi.org/10.1145/2486001.2486033

[3] Y. R. Chien. 2015. Design of GPS Anti-Jamming Systems Using Adaptive Notch Filters. *IEEE Systems Journal* 9, 2 (June 2015), 451–460. https://doi.org/10.1109/JSYST.2013.2283753

[4] T. C. Clancy. 2011. Efficient OFDM Denial: Pilot Jamming and Pilot Nulling. In *2011 IEEE International Conference on Communications (ICC)*. 1–5. https://doi.org/10.1109/icc.2011.5962467

[5] B. DeBruhl and P. Tague. 2013. How to jam without getting caught: Analysis and empirical study of stealthy periodic jamming. In *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*. 496–504. https://doi.org/10.1109/SAHCN.2013.6645021

[6] Philip K. Dick. 1968. *Do Androids Dream Of Electric Sheep?* Ballantine Books.

[7] Ettus Research. 2019. X300/X310 - Ettus Knowledge Base. https://kb.ettus.com/X300/X310#Option:_GPS_Disciplined.2C_Oven-Controlled_Oscillator_.28GPSDO.29 Accessed 2019-01-20.

[8] Yanming Feng and Jinling Wang. 2008. GPS RTK performance characteristics and analysis. *Journal of Global Positioning Systems* 7, 1 (2008), 1–8.

[9] C. Fernández–Prades, J. Arribas, P. Closas, C. Avilés, and L. Esteve. 2011. GNSS-SDR: An Open Source Tool For Researchers and Developers. In *Proc. of the ION GNSS 2011 Conference*. Portland, Oregon.

[10] Nirnimesh Ghose, Loukas Lazos, and Ming Li. 2017. HELP: Helper-Enabled In-Band Device Pairing Resistant Against Signal Cancellation. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 433–450. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/ghose

[11] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. 2011. They Can Hear Your Heartbeats: Non-invasive Security for Implantable Medical Devices. In *Proceedings of the ACM SIGCOMM 2011 Conference (SIGCOMM '11)*. ACM, New York, NY, USA, 2–13. https://doi.org/10.1145/2018436.2018438

[12] Alan Grant, Paul Williams, Nick Ward, and Sally Basker. 2009. GPS Jamming and the Impact on Maritime Navigation. *Journal of Navigation* 62, 2 (2009), 173–187. https://doi.org/10.1017/S0373463308005213

[13] Todd Humphreys. 2017. *Springer Handbook of Global Navigation Satellite Systems*. Springer International Publishing, Cham, 469–503. https://doi.org/10.1007/978-3-319-42928-1_16

[14] IGS. [n. d.]. IGS Products – GPS Satellite Ephemerides / Satellite & Station Clocks. http://www.igs.org/products. Accessed: 2016-12-7.

[15] osqzss. 2018. Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim Accessed 2019-01-20.

[16] M. Petracca, M. Vari, F. Vatalaro, and G. Lubello. 2012. Performance evaluation of GSM robustness against smart jamming attacks. In *2012 5th International Symposium on Communications, Control and Signal Processing*. 1–6. https://doi.org/10.1109/ISCCSP.2012.6217797

[17] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun. 2011. Investigation of Signal and Message Manipulations on the Wireless Channel. In *Proceedings of the 16th European Conference on Research in Computer Security (ESORICS'11)*. Springer-Verlag, Berlin, Heidelberg, 40–59. http://dl.acm.org/citation.cfm?id=2041225.2041229

[18] M. L. Psiaki and T. E. Humphreys. 2016. GNSS Spoofing and Detection. *Proc. IEEE* 104, 6 (June 2016), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

[19] Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun. 2016. SPREE: A Spoofing Resistant GPS Receiver. In *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking (MobiCom '16)*. ACM, New York, NY, USA, 348–360. https://doi.org/10.1145/2973750.2973753

[20] J.S. Subirana, J.M.J. Zornoza, M. Hernández-Pajares, European Space Agency, and K. Fletcher. 2013. *GNSS Data Processing*. ESA Communications.

[21] US Department of Defence. 2008. GPS SPS Performance Standard. Online: https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

[22] David L. M. Warren and John F. Raquet. 2003. "Broadcast vs. precise GPS ephemerides: a historical perspective". *GPS Solutions* 7, 3 (2003), 151–156. https://doi.org/10.1007/s10291-003-0065-3

[23] Kyle D. Wesson, Jason N. Gross, Todd E. Humphreys, and Brian L. Evans. 2017. GNSS Signal Authentication via Power and Distortion Monitoring. arXiv:arXiv:1702.06554

[24] Matthias Wilhelm, Ivan Martinovic, Jens B. Schmitt, and Vincent Lenders. 2011. Reactive Jamming in Wireless Networks: How Realistic is the Threat?. In *Proceedings of the Fourth ACM Conference on Wireless Network Security (WiSec '11)*. ACM, New York, NY, USA, 47–52. http://dl.acm.org/authorize?431905

[25] L. Xiao, T. Chen, J. Liu, and H. Dai. 2015. Anti-Jamming Transmission Stackelberg Game With Observation Errors. *IEEE Communications Letters* 19, 6 (June 2015), 949–952. https://doi.org/10.1109/LCOMM.2015.2418776

[26] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang. 2006. Jamming sensor networks: attack and defense strategies. *IEEE Network* 20, 3 (May 2006), 41–47. https://doi.org/10.1109/MNET.2006.1637931

[27] S. Yubo, Z. Kan, Y. Bingxin, and C. Xi. 2010. A GSM/UMTS Selective Jamming System. In *2010 International Conference on Multimedia Information Networking and Security*. 813–815. https://doi.org/10.1109/MINES.2010.172