JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

EXAMINING THE COUNTERMEASURES OF GPS SPOOFING ATTACKS

Sunny Arora[1], Amit Tuteja[2]
[1,2]Guru Kashi University, Talwandi Sabo

Abstract

Today, GPS is a necessary component of our navigation and positioning systems. In today's world, every aircraft, container ship, vehicle, and even mobile phone is equipped with GPS. Because GPS is such a frequently used and important tool, it has become a tempting target for criminals and hackers. The expansion of data communication needs today is pushing wireless networks to their limits. Spectrum is the most significant constraint to wireless network capacity. We created forged GPS coordinates and sent them to the drone, causing it to divert from its intended path while avoiding detection by the drone's standard control systems. However, before attacking the drone, we ran a preliminary attack test on a GPS receiver to ensure that our GPS attack framework was viable. We established a practical framework for better management of drone movement in this project, based on a thorough study of consumer drone challenges. The proposed attack has been quite successful in our lab surroundings; but, due to device limitations, field circumstances, and other factors beyond our control, such as wind speed, there are significant practical hurdles in field experiments.

Keywords: countermeasure, GPS, spoofing, attack, etc

1. INTRODUCTION

Today, GPS is a necessary component of our navigation and positioning systems. In today's world, every aircraft, container ship, vehicle, and even mobile phone is equipped with GPS. Because GPS is such a frequently used and important tool, it has become a tempting target for criminals and hackers. Because GPS signals are sent from satellites that are 1300 miles distant, the atmosphere in between contains biases and inaccuracies, which cause GPS signals to be inaccurate. GPS communication is also harmed by these biases and mistakes. Satellite signals, on the other hand, are so weak that they are susceptible to both intentional and inadvertent radio frequency interference. To start a spoofing attack, the spoofer sends out counterfeit signals that are code-phase synced with original GPS signals but at a low enough power to get lost in the noise. The spoofer then increases the spoofing signal's power until it is somewhat greater than that of authentic transmissions. Spoofer now has control of the victim receiver's tracking loops, allowing him to gradually separate the spoofing signals from the actual GPS signals. Once the spoofing signals have moved the receiver 2 microseconds in time or 600 metres away from the authentic navigation solution, the victim receiver can be said to be entirely possessed by the spoofer. A synchronous spoofing attack is one in which the spoofer attempts the attack in accordance with the conditions described above; otherwise, it is an asynchronous spoofing attack, as shown in Fig. 1.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

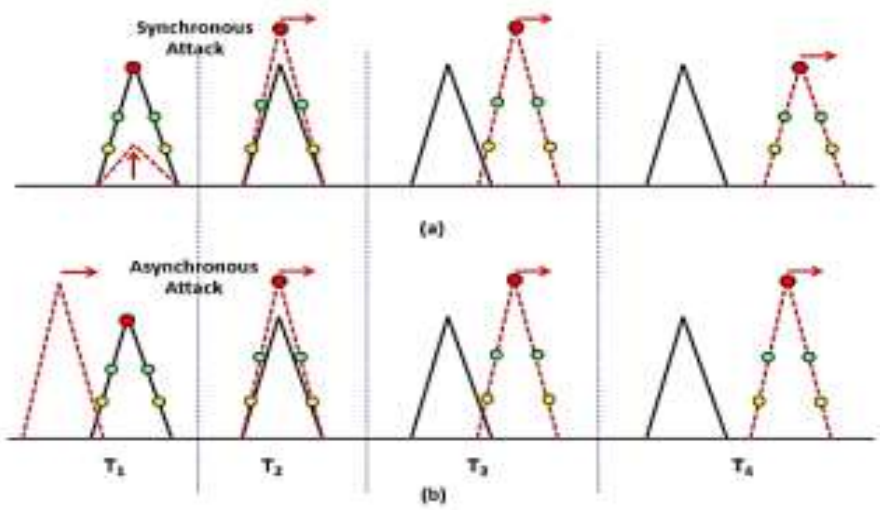

Figure 1: (a) Synchronous spoofing attack, (b) Asynchronous spoofing attack

- **Spoofing Attack Vulnerability in GPS-Reliant Infrastructure**

Given the ease with which a spoofing source can affect some GPS receivers, it's reasonable to assume that GPS-dependent infrastructure is likewise vulnerable to spoofing assaults, given that it's directly connected to GPS. The electricity grid and the telecommunication network, for example, both rely on GPS time-reference receivers to get accurate and exact timing. Many additional applications that require position, timing, or velocity rely on GPS services as well. Spoofing a GPS receiver is the deliberate and intentional transmission of fake/false GNSS signals with the goal of deceiving a GNSS receiver into retrieving incorrect Position, Velocity, and Time (PVT) data. Unlike jamming, the primary goal of a spoofing attack is to compel a GNSS receiver to chase down phoney GNSS signals in order to provide an incorrect navigational solution.

1.1 In Database-Driven Cognitive Radio Networks, a Location Spoofing Attack and Its Countermeasures

The expansion of data communication needs today is pushing wireless networks to their limits. Spectrum is the most significant constraint to wireless network capacity. Military communications, broadcast television, WiFi, cellular systems, and a variety of other uses compete for spectrum. The accessible spectrum is currently licensed to these various purposes. Some applications, such as cellular systems, have grown far more quickly than others, such as broadcast radio and broadcast television. As a result, some spectrum bands are overcrowded, while others are underutilised. Cognitive radio networks (CRNs) with dynamic spectrum access can help to alleviate this spectrum imbalance. There are two types of users in CRNs: primary users (PUs) and secondary users (SUs) (SUs). PUs always has full spectrum access anytime they need it. The spectrum can only be used by SUs if they don't interact with the PUs. TV White Spaces (TVWS) and the 3550-3650 MHz spectrum are two potential applications (3.5 GHz Band). The term "TVWS" refers to any location's unused television channels. The FCC published a study in November 2008 outlining the requirements for SUs to operate in licensed TV bands. A reliable geolocation database will be used to assign spectrum to SUs so that they do not interfere with licenced PUs, according to the regulations. The FCC proposed a new Citizens Broadband Service in the 3.5 GHz Band in December 2012. To make better use of radio spectrum, the Citizens Broadband Service uses database-driven dynamic spectrum access and small cell technology1.

2. REVIEW OF THE LITERATURE

Mukhtar Ahmad and Muhammad Akhtar (2019) Because GPS signals are faint; they are susceptible to in-band interference when broadcast over wireless channels. Even low-power interference can induce GPS spoofing,

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

which can lead to disaster. Spoofing and anti-spoofing strategies are growing challenges in the realm of GPS for the reasons stated above. Spoofing works because the targeted receiver is unaware of it. In general, the spoofer attempts to produce or replicate actual GPS signals in order to deceive a GPS receiver. Because of advancements in SDR (software defined receiver) technology, spoofing is becoming easier and less expensive.

Kexiong Zeng, Sreeraksha Ramesh, and Yaling Yang (2014) Database-driven cognitive radio networks (CRNs), which comprise white space networks in TV bands (TV band CRNs) and newly proposed small cell networks in 3.5 GHz, have been mandated by the FCC (3.5 GHz CRNs). A secondary user (SU) in a database-driven CRN queries the database for available spectrum at its location. This, however, creates a serious vulnerability to GPS spoofing assaults. An adversary compromises the GPS localization system of SUs in this attack, causing SUs to query the database with bogus positions and obtain wrong spectrum information. We investigate the impact of GPS spoofing attacks in database-driven CRNs and present spoofing attack detection and countermeasure strategies in this work. This is the first investigation of the impact and mitigation of GPS spoofing attacks in database-driven CRNs that we are aware of.

Ali Jahromi, Ali Broumandan, J. Nielsen, and Gérard Lachapelle, (2012) By creating many fake correlation peaks and boosting the noise floor, spoofing sources can successfully disturb a GPS receiver during the acquisition phase. Such false correlation peaks can trick the GPS receiver into picking up spoofer generated signals instead of genuine signals. In addition, the spoofer can raise the receiver noise floor to bury the genuine signals in the noise while simultaneously generating correlation peaks with amplitudes that are consistent with reasonable C/N0 assumptions. The main focus of this research is on determining whether the GPS spoofer countermeasure is less successful during acquisition when the GPS receiver uses C/N0 discrimination. While the C/N0 discrimination is ineffective, the receiver may measure the absolute power of the correlation peaks with a minor circuit adjustment, which is a successful way of detecting and discriminating spoofer sources. When compared to C/N0 monitoring techniques, it will be shown that using absolute power monitoring techniques significantly minimizes the vulnerability zone of the receiver.

Nils Ole Tippenhauer, Christina Pöpper, Kasper Rasmussen, and Srdjan Capkun (2011) for localization, navigation, and time synchronisation, an increasing number of wireless apps rely on GPS signals. However, civilian GPS signals are known to be vulnerable to spoofing attempts, which cause GPS receivers in range to believe they are located somewhere other than where they actually are. The conditions for successful GPS spoofing assaults on individuals and groups of victims using civilian or military GPS receivers are investigated in this study. We're particularly interested in determining where the attacker must emit signals and with what precision in order to properly spoof the receivers. We'll show, for example, that any number of receivers can be easily faked to one arbitrary location; yet, when spoofing a group of receivers while keeping their constellation, the attacker is limited to only a few transmission sites. We also look into the practical implications of a satellite-lock takeover, in which a victim receives faked signals after being locked on to authentic GPS signals. We conduct a series of experiments with a civilian GPS signal generator to determine the minimum precision of the attacker's spoofing signals required for covert satellite-lock takeover.

3. OBJECTIVES

- To find out Database-Driven Cognitive Radio Networks, a Location Spoofing Attack and Its Countermeasures.
- To analyze Moving Position Spoofing.

4. RESEARCH METHODOLOGY

4.1 Hardware Platform

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

We created forged GPS coordinates and sent them to the drone, causing it to divert from its intended path while avoiding detection by the drone's standard control systems. However, before attacking the drone, we ran a preliminary attack test on a GPS receiver to ensure that our GPS attack framework was viable. Figure 2 depicts the hardware setup for the test. A GPS receiver must first be locked to real GPS satellites in order to display its true location. After that, we downloaded broadcast ephemeris (BRDC) data from NASA's CDDIS website, created a bitstream of spoofing GPS positions with GPS-SDR-SIM, and sent the signal through bladeRF. The spoofing signal then replaced the signal from the satellites at a GPS receiver, causing the receiver's reading to reflect the fabricated position.

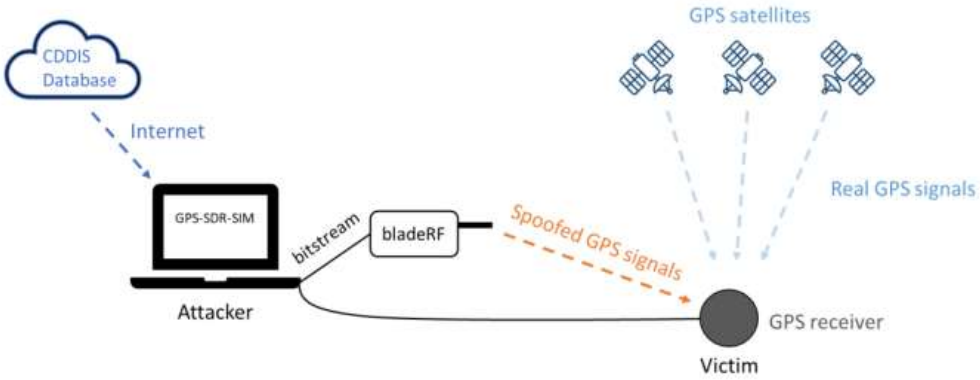

Figure 2: Setup for attacking a GPS receiver

We tested GPS spoofing on a drone after our attacking approach was validated. Figure 3 depicts the configuration. In the testing, we employed two computers: one as an attacker, generating a spoofing GPS signal and transmitting it to the drone, and the other as an observer, reading and recording the drone's status. The attacker also served as a controller, sending control commands to the drone to launch it or allow it to undertake a mission. For data connection, the two PCs were connected to the drone over a Wi-Fi network and used the MAVLink protocol. We could modify the drone's flying path by delivering intricately created GPS position trajectories after the spoofing signal took over the GPS fix.

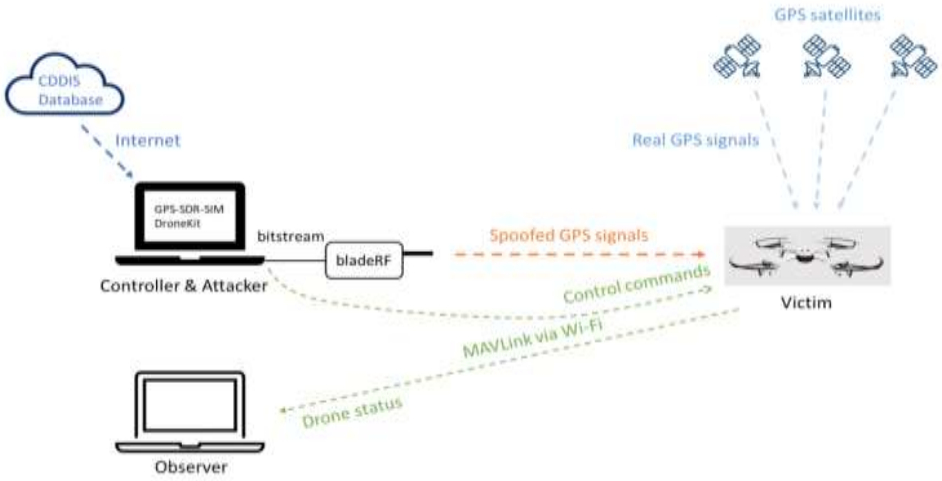

Figure 3: Setup for attacking a drone

5. RESULT AND DISCUSSION

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

- **Moving Position Spoofing**

We might also construct places in a moving trajectory and allow the receiver to virtually walk along it by following the procedures below:

✓ In Google Maps, draw a route (see Figure 4) and save it as a KML file, which is used to display geographic data in an Earth browser (such as Google Earth). It is based on the XML standard and uses a tag-based structure with nested components and attributes.

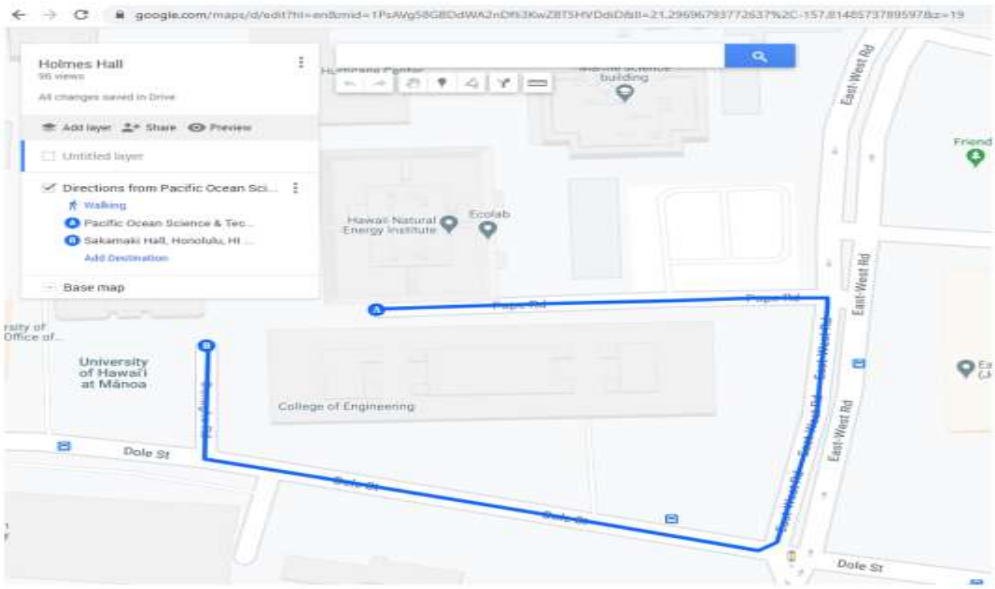

Figure 4: A route around Holmes Hall in Google Maps

✓ Using SatGen Trajectory generation, convert it to an NMEA file. Figure 5 shows the software interface, where we set the maximum speed to 20 km/s and the output rate to 10 Hz.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

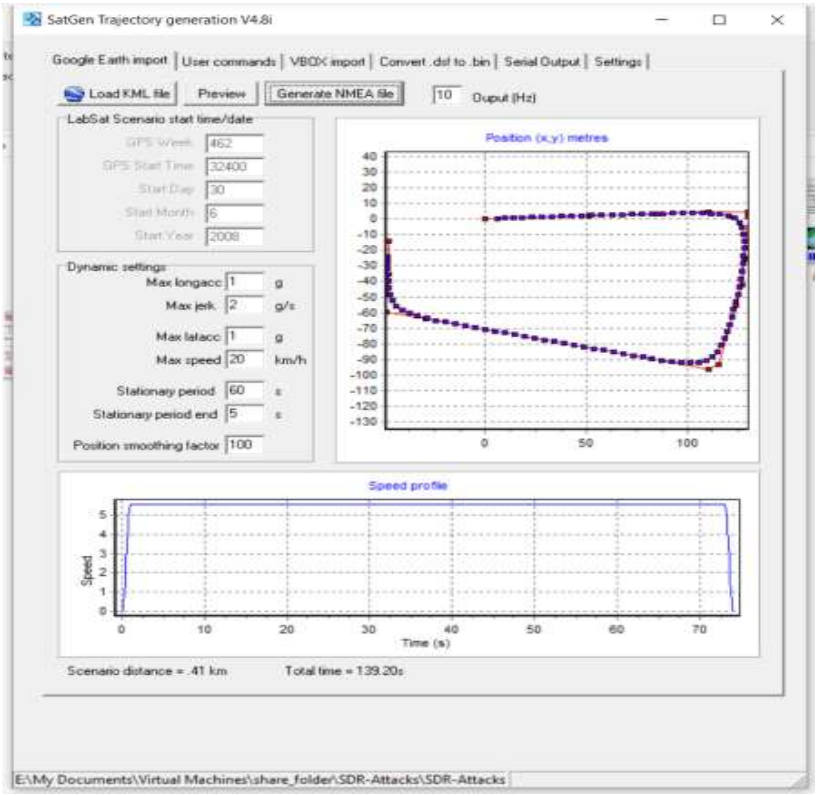

Figure 5: Generate NMEA file in SatGen Trajectory generation. (Note the Y-axis label is m/s)

- ✓ Using gps-sdr-sim, create the bitstream.
- ✓ Use bladeRF to send the bitstream. The script is identical to the fixedposition test's.

As illustrated in Figure 6, we plotted the broadcast and received GPS routes. We also determined the maximum X-Y coordinate and height position deviations, which are 7.7m and 35.9m, respectively.

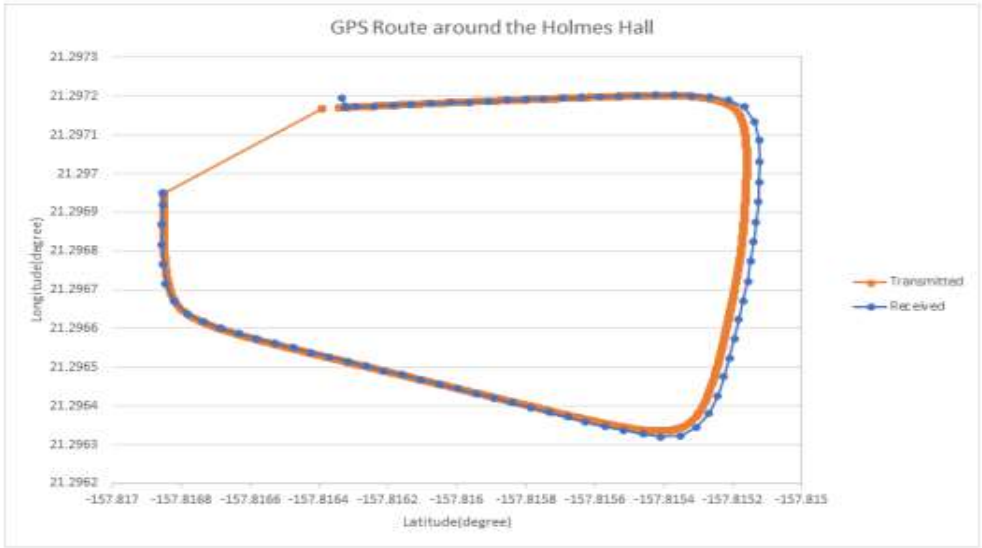

Figure 6: GPS route around the Holmes Hall

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

Encrypted military-grade GPS coding could be used as a countermeasure to the planned GPS spoofing attack. Attackers won't be able to construct such encrypted code using open-source algorithms; therefore spoofing GPS coordinates will be difficult. Drone motion may be tracked and verified using wireless localization technology, and deviations in drone motion can be detected. In the event that GPS fails, calibration can be done using other navigation technologies such as high-precision inertial navigation, vision navigation, or even manual controls.

6. CONCLUSION

Most consumer drones rely on GPS signals to detect their present positions, navigate to their destinations via a sequence of waypoints, and perform the popular return-home feature. However, because civilian GPS is the most extensively used positioning and time synchronisation system for many unmanned auto-controlled systems, the GPS input of a consumer drone is an obvious weakness. A GPS device, in particular, receives signals from the GPS satellite constellation and calculates 3-dimensional position, velocity, and high-precision time. Although simple GPS spoofing has been done in a variety of scenarios, the most of them are brute-force attacks with no exact control, as far as we know. We established a practical framework for better management of drone movement in this project, based on a thorough study of consumer drone challenges. The proposed attack has been quite successful in our lab surroundings; but, due to device limitations, field circumstances, and other factors beyond our control, such as wind speed, there are significant practical hurdles in field experiments.

REFERENCES

1. Ahmad, Mukhtar & Akhtar, Muhammad. (2019). Impact and Detection of GPS Spoofing and Countermeasures against Spoofing.

2. Zeng, Kexiong & Ramesh, Sreeraksha & Yang, Yaling. (2014). Location spoofing attack and its countermeasures in database-driven cognitive radio networks. 202-210. 10.1109/CNS.2014.6997487.

3. Jahromi, Ali & Broumandan, Ali & Nielsen, J. & Lachapelle, Gérard. (2012). GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements. International Journal of Satellite Communications and Networking. 30. 10.1002/sat.1012.

4. Tippenhauer, Nils Ole & Pöpper, Christina & Rasmussen, Kasper & Capkun, Srdjan. (2011). On the requirements for successful GPS spoofing attacks. 75-86. 10.1145/2046707.2046719.

5. Daniele Borio, Fabio Dovis, Heidi Kuusniemi, and Letizia Lo Presti,"Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers,'' in proceedings of IEEE, Vol. No. 6, June 2016.

6. A. Jafarnia-Jahromi, T. Lin, A. Broumandan, J. Nielsen, and G. Lachapelle, "Detection and mitigation of spoofing attack on a vector based tracking GPS receiver," in Proceedings of the International Technical Meeting of The Institute of Navigation, Newport Beach, Calif, USA, January 2012.

7. Kyle Wesson, Daniel Shepard, and Todd Humphreys,'' Straight Talk on Anti-Spoofing Securing the Future of PNT,'' GPS World Magazine, vol. 23, no. 1, pp. 32-63, 2012.

8. Alexander RÜGAMER and Dirk KOWALEWSKI, '' Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!''.

9. Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gerard Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," Hindwi Publishing Corporation International Journal of Navigation and Observation Volume 2012, Article ID 127072, 16 pages.

ISSN- 2394-5125 VOL 08, ISSUE 03, 2021

10. Günther, Christoph. (2014). A Survey of Spoofing and Counter-Measures. Navigation. 61. 10.1002/

11. navi.65.