Location Robustness in 3.5 GHz Cognitive Radio Networks

Kexiong Zeng and Yaling Yang
Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Email: {kexiong6, yyang8}@vt.edu

Abstract—The recent FCC ruling has proposed 3.5 GHz database-driven cognitive radio networks (CRNs) in which the database relies on a base station to determine his location to query the database for available spectrum. However, this creates a critical loophole for mounting GPS-spoofing attack, which can potentially result in interference with critical incumbent users. The adversary attacks base stations’ GPS which results in base stations querying the database with false location and obtaining incorrect available spectrum information. In this paper, we describe the impact of a GPS-spoofing attack on 3.5 GHz database-driven CRNs and propose multi-radio localization method to detect such attack. We also implement and evaluate the performance of our detection mechanism. To the best of our knowledge, this is the first paper to examine the impact of a GPS spoofing attack on 3.5 GHz database-driven CRNs and present a detection mechanism for the same.

I. INTRODUCTION

There is an explosion of data and video being carried on wireless networks today which is stretching the capacity limits of wireless networks. The principal limiting factor for the capacity of wireless networks is spectrum. Military communications, broadcast TV, WiFi, cellular systems and many such applications all compete for spectrum. Currently, the spectrum available is licensed to these different applications. However, the growth of applications like cellular has far outgrown those of broadcast TV or radio for instance. This leads to overcrowding in specific bands and under-utilization of other spectrum bands. Dynamic Spectrum Access (DSA) is a technology that helps to ease this overcrowding and under-utilization.

In December 2012, the FCC adopted a Notice of Proposed Rulemaking (NPRM) that proposed to make available at least 100 megahertz of spectrum in the 3.5 GHz Band for shared, commercial uses, including small cell networks. The 3.5 GHz NPRM proposes a three-tier, license-by-rule authorization framework that would facilitate rapid broadband deployment while protecting existing incumbent users of the 3.5 GHz Band. Under this proposal, access to the 3.5 GHz Band would be governed by a dynamic Spectrum Accessing System, building on the TV White Spaces database concept.

With FCC laying stress on database-driven methods, it is imperative to examine the security threats in such a network. One critical security loophole is caused by the fact that this method relies on a base station obtaining its location information from Global Positioning System (GPS). GPS, although originally introduced by the US military, is a very essential part of many civilian applications today. The use of GPS in critical applications motivated a lot of research on GPS security.

In 2001, the U.S. Department of Transportation conducted an inquiry into the vulnerability of US Transportation infrastructure to disruptions in civilian GPS [1]. The study, also called Volpe report, identified jamming and spoofing as some of the vulnerabilities of GPS receivers. The spoofing attack is far more malicious than a simple jamming attack as it is not so easy to detect and the adversary can also inject misleading information which can lead the GPS receiver to compute its location coordinates incorrectly. Although Edwin L. Key mentions several mechanisms to mitigate spoofing [2], the Volpe report identifies that none of the countermeasures have been implemented in commercial GPS receivers. Thus, off-the-shelf GPS receivers are indeed vulnerable to spoofing attack and this is agreed upon by [3].

 Particularly, successful spoofing of commercial off-the-shelf standard GPS receiver has been demonstrated in [3], [4]. With the development of platforms such as USRPs, it has become quite easy to build GPS simulators. GPS simulators generate signals similar to actual GPS signals, but allow for complete control over aspects like date, time and location. In [4], a WelNavigate GS720 GPS signal simulator along with two GPS amplifiers is used to attack a GPS receiver in a truck. In [3], the authors discuss a software-defined GPS receiver-spoofer and use this to successfully demonstrate a spoofing attack. Apart from numerous demonstrations of the spoofing attack, there has also been an in-depth analysis about the effect of a GPS spoofing attack on a group of receivers. In [5], the authors prove that any number of receivers can easily be spoofed to one arbitrary location by a single attacker with an omnidirectional antenna.

In this paper, we consider the geolocation security issues in the context of 3.5 GHz database-driven small cell networks, which consists of low-powered wireless base stations and clients associated with the base stations. Base stations have to register in the database and provide accurate location information before operate. The database assign available spectrum to base stations in a manner that ensures that such devices would not interfere with incumbents, like existing radar or satellites. We propose a GPS spoofing attack on such a network which result in serious interference with critical incumbent users. In order to detect this attack, we propose a multi-radio localization scheme to verify the authenticity of base stations’ GPS reported locations. Experiment results show our detection mechanism are effective to detect GPS-spoofing attacks. The contributions of this work are as follows:

• We discuss the impact of GPS spoofing attack on 3.5 GHz database-driven CRNs.
We propose a multi-radio mechanism to detect GPS-spoofing attacks.

We evaluate our attack detection scheme in practical experiments.

To the best of our knowledge, this is the first paper to examine the impact of a GPS-spoofing attack on 3.5 GHz database-driven CRNs and present a detection mechanism for the same.

The rest of the paper is organized as follows. We introduce GPS-spoofing attack model in Section II, and propose spoofing attack detection mechanism as well as provide evaluation results in Section III.

II. ATTACK MODEL

In this section, we give an overview of the geolocation security loophole that can be utilized by adversaries to launch different kinds of attacks on 3.5 GHz database-driven CRNs.

A. GPS Spoofing Attack

In this paper, we consider a single attacker equipped by an omni-directional antenna as described in [5]. The idea is that if a single transmission antenna is used by an attacker, then all victims receive signals with the same time difference. As the time difference of arrival determines the location computed, all the receivers can only be spoofed to the same location, say, \(L'\). Figure 1 illustrates this idea. Base stations within the attackers range get spoofed to location \(L'\).

![Fig. 1. Single-attacker GPS-spoofing attack.](image)

B. Geolocation Security Loophole

Based on the proof that a single attacker can easily spoof a group of GPS receivers to one arbitrary location \(L'\), we find a geolocation security loophole in 3.5 GHz database-driven CRNs. As Figure 2 shown, there are large exclusion zones where incumbent users, like high powered Department of Defense (DoD) radars are using 3.5 GHz band and non-exclusion zones where incumbents are inactive. An attacker can either spoof the base stations from exclusion zones to non-exclusion zones or in the opposite way. The spoofed base station submits its GPS location \(L'\) to the database to complete the mandatory registration. Because the database and base station are both unaware of this spoofing attack, the database will response the base station with the spectrum availability based on \(L'\). Therefore, such an attack can either result in dangerous interference with existing incumbents or false deny of service to base stations.

![Fig. 2. Exclusion zones and non-exclusion zones](image)

III. SPOOFING ATTACK DETECTION

In this section, we propose a multi-radio localization method to detect GPS-spoofing attacks. Our method leverages the fact that a base station is usually also a software defined radio (SDR), which can tune to different wireless systems operating at a wide range of spectrum bands through a simple switch of software. Thus, in our scheme, a base station listen to the signals emitted by existing infrastructures (i.e. TV towers, WiFi access points and FM towers) to compute a backup location. This backup position can then be used to verify GPS location, detect GPS-spoofing attack and also be used as a backup location when GPS are under spoofing attacks.

A. Television-Based Positioning Technology

Recently, Rosum company has developed a chip called “Alloy” that can use plain old TV broadcast signals to accurately localize people and objects. As illustrated in Figure 3, Rosum TV-positioning technology utilizes the time of arrival of TV broadcast signals and the locations of corresponding terrestrial broadcast television infrastructures to calculate location. With support for a variety of types of TV signals, Alloy is able to provide <150 meters accuracy even in the worst case [6]. Terrestrial broadcast TV signals are high-power, low-frequency signals that easily penetrate buildings and urban areas. Furthermore, TV signals have a quite large bandwidth (i.e. from 54 MHz to 890 MHz), which makes them robust to jamming or spoofing attacks.

If base stations operating on 3.5 GHz are equipped with the Alloy chips, they can use the location calculated by TV-positioning technology to verify the GPS location. When a mismatch between these two locations is detected, the base station raise a suspicion on GPS-spoofing attack. By aggregating multiple neighboring base stations’ suspicion reports together, the existence of GPS-spoofing attack can be detected reliably. Besides, TV-positioning technology is required when base stations are placed indoor where GPS cannot work. Such a solution can not only detect the GPS-spoofing attack but also provide indoor localization ability. Therefore, TV localization can be a primary solution for GPS-spoofing attack detection.
B. WiFi Beacon Signal Decoding

A secondary spoofing attack detection method is WiFi beacon signal decoding. As software defined radios, base stations are able to decode IEEE 802.11 packets transmitted by surrounding WiFi access points with no extra hardware. If a base station successfully decodes any WiFi beacon signals, he looks up the decoded SSID and MAC address in pre-stored WiFi map to locate these WiFi access points. A GPS-spoofing attack will be detected if the GPS-reported location is outside of the transmission range of the specific WiFi access points. This detection mechanism is fairly effective in high WiFi-density areas, like indoor and urban areas. Based on the source code provided by the authors of [7], we have re-implemented a GNURadio-based IEEE 802.11 a/g/p receiver on USRP N210. As shown in Figure 4, our experimental setup consists of a USRP N210 motherboard, a SBX daughterboard and two VERT2450 antennas manufactured by Ettus Research.

We run the GNURadio WiFi receiver and set the sampling rate to 20 MHz and the center frequency to 2.437G. The results are illustrated in Figure 5. We successfully decode beacon signals from two nearby WiFi access points whose SSIDs are “VT-Wireless” and “CONNECTtoVT-Wireless”. By comparing the SSIDs and MAC address with the fingerprints pre-stored in WiFi map, we know the receiver is in the Durham Hall at Virginia Tech. Further, we can verify that the GPS location is true only if it is inside or near Durham Hall. Otherwise, the receiver is possibly under a GPS-spoofing attack.

C. FM Broadcast Signal Localization

It is likely that a base station neither has Rosum’s Alloy chip nor does he receives any surrounding WiFi beacon signals. In order to handle such a situation, we need a backup localization method to detect GPS-spoofing attack. FM radio localization is an ideal backup plan because FM signals are widely available both indoors and outdoors. In this paper, we developed a two-phase localization system using FM radio received signal strength indicator (RSSI). In the first phase, we collect realistic FM RSSI fingerprints by a commercial spectrum analyzer and store them in a database. In the second phase, the receiver estimates his location by comparing the measured receiving signal power and the pre-stored RSSI fingerprints.

1) Data Collection: We perform the experiment in Blacksburg and Christiansburg with an area of around 86.25 km$^2$. We select 26 locations shown as the red balloons in Figure 6. To record numerical RSSI of FM channels, we use a Tektronix MDO4104-6 Mixed Domain Oscilloscope and a v-shaped “rabbit ear” FM antenna, as shown in Figure 7. We take measurements of 17 FM channels at each test position.

2) Localization Algorithm: In this paper, we use the same positioning algorithm proposed in [8]. Our task is to estimate the locations from the pre-stored reference points. So we use likelihood of each reference position to calculate estimated location represented by numerical latitude and longitude. In this
way, the localization problem can be formulated as follows:

\[ \mathcal{L} = \sum_{k=1}^{n} L_k \cdot P_{\text{norm}}(X|C_k) \]  

(1)

where

\[ P_{\text{norm}}(X|C_k) = \frac{P(X|C_k)}{\sum_{k=1}^{n} P(X|C_k)} \]  

(2)

In Equation 1, \( \mathcal{L} \) is the localization output represented by numerical latitude and longitude. \( L_k \) is the coordinate of \( k \)th reference position. As shown in Equation 2, \( P_{\text{norm}}(X|C_k) \) is the normalized likelihood that observation RSSI vector \( X \) is measured in reference location \( C_k \). We model the RSSI for each reference point as a Gaussian distribution such that likelihood \( P(X|C_k) \) is numerically computable.

3) Performance Evaluation: Figure 8 shows how error distribution (i.e. mean plus standard deviation) varies by increasing the number of FM channels. In order to obtain a better localization performance, we always select the strongest FM channels at each test position to calculate estimated location. As you can see, we are able to achieve 50-meter accuracy with 8 strongest FM channels. Hence FM localization can be used as a backup spoofing attack detection method when neither TV positioning nor WiFi beacon signals are available. If the system doubts a base station’s GPS location, he asks the base station to measure the RSSI of a number of strongest local FM channels indicated by the database. If the GPS location mismatches the position calculated by FM localization algorithm, a GPS-spoofing attack is detected.

IV. CONCLUSION

In this paper, we study the impact of GPS-spoofing attack on a 3.5 GHz database-driven CRNs and propose a multi-radio location verification mechanism to detect such an attack. We also implement and evaluate our detection mechanism by practical experiments.

REFERENCES


