Location Robustness in Database-Driven White Spaces Network

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

***Abstract*—The recent FCC ruling has enforced database-driven white spaces network (WSN) in which the database relies on a secondary user (SU) 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 primary user (PU) interference. The adversary attacks SUs' GPS which results in SUs querying the database with false location and obtaining incorrect available spectrum information. In this paper, we examine the impact of a GPS spoofing attack on database-driven WSN, propose a spoofing attack detection mechanism and provide simulation results of the scheme. We also propose an analytical model for the detection mechanism and derive an upper bound for the convergence time of our model. To the best of our knowledge, this is the first paper to examine the impact of a GPS spoofing attack on database-driven WSN and present a detection mechanism for the same.**

I. Introduction

Today's explosion of data communication needs is stretching the capacity limit 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, some applications like cellular systems, have grown much faster than others, such as broadcast radio and broadcast TV. This leads to overcrowding in some bands and underutilization of other spectrum bands. Dynamic Spectrum Access (DSA) is a technology that helps to ease this imbalance in spectrum utilization.

A potential application for using DSA to improve spectrum utilization is in TV White Spaces (TVWS). TVWS refers to the unused TV channels in any location. In November 2008, the FCC issued a report that specifies the requirements for secondary users (SUs) to operate in licensed TV bands. According to the requirements, a trusted geolocation database will be used to assign spectrum to SUs so that they will impose no interference to licensed users.

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 SU obtaining its location information from Global Positioning System (GPS). GPS, although originally introduced by the US military, is an essential part of many civilian applications today. Its security vulnerability to attacks is well-known in these application areas. For example, 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 because it is not so easy to detect and the adversary can also inject misleading information to cause the GPS receiver to compute incorrect location. Although works by Edwin L. Key proposed several countermeasure mechanisms for GPS spoofing [2], the Volpe report pointed out that none of the countermeasures have been implemented in commercial GPS receivers. Thus, it is well recognized in the GPS community that off-the-shelf GPS receivers are very vulnerable to spoofing attack.

Successful spoofing of commercial off-the-shelf standard GPS receiver has been demonstrated in previous works. With the development of platforms such as USRPs, it has become quite easy to build GPS simulators to launch such spoofing attack. GPS simulators generate signals similar to actual GPS signals, but allow for complete control over aspects like date, time and location. In [3], the authors discuss a software-defined GPS receiver-spoofer and use this to successfully demonstrate a spoofing attack. In [4], a WelNavigate GS720 GPS signal simulator along with two GPS amplifiers is used to attack a GPS receiver in a truck. 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. Tippenhauer et al. prove that any number of receivers can easily be spoofed to one arbitrary location by a single attacker [5].

In this paper, we focus on the geolocation security issues in the context of a database-driven and infrastructure-based WSN, which consists of base stations (BSs) and SU clients associated with the BSs. Through simulation, we demonstrate that GPS spoofing can cause serious PU interference. To countermeasure GPS spoofing attacks, we propose a location verification mechanism to verify the authenticity of SUs' GPS location report. We developed a mathematical analytical model for our proposed detection solution to analyze its convergence speed. Simulation results show that our mechanism can achieve nearly 100% accuracy in most cases except for fairly low SU density situation.

The contributions of this work are as follows:

- We examine the impact of GPS spoofing attack on a database-driven WSN.
- We propose a mechanism to detect GPS spoofing attacks and determine victim SUs, as well as evaluate the scheme in simulation.
- We propose an analytical model for spoofing detection scheme and use spectral analysis to derive an upper bound for convergence time.

To the best of our knowledge, this is the first paper to

978-1-4799-2661-9/14/$31.00 ©2014 IEEE

examine the impact and propose a countermeasure for GPS spoofing attack on database-driven WSN.

The rest of the paper is organized as follows. We introduce and simulate GPS spoofing attack model in Section II, propose spoofing attack detection mechanism in Section III, and present evaluation in Section IV. Finally, Section V concludes the paper.

II. Attack Model

In this section, we first study the framework for simulating the attack model, then identify metrics for studying the impact of the attack and finally present simulation results for the attack.

A. GPS Spoofing Attack

As outlined in the previous section, we assume that the GPS spoofing attack can be launched on off-the-shelf GPS receivers, which do not as yet have any security mechanisms for protecting against these attacks. In the presence of an attacker, the SU's location can be spoofed to a false location L'. As the database and SU are both unaware of this spoofing attack, database assigns the spoofed SU an available channel at L'. This, however, does not protect the PUs who are active in the SU's true location, L. In order to examine the impact, we consider a 16km-radius cell containing n SUs (uniformly distributed). We introduce an attacker who controls a single antenna that he can position anywhere and create a random false location L' within the cell. We assume that the attacker, A, has a spoofing range capability of R and hence all SUs within this radius have false GPS location L'.

Here we consider that the spoofed location L' is within the cell because otherwise the attack is trivial to detect. For instance, the BS can easily detect such an attack as a SU associates with a BS but his GPS location is outside the BS's cell.

B. Database and Spectrum Allocation

In order to evaluate the impact of GPS spoofing attack on a database-driven WSN, we also need to define the model of such a network. We use WhiteSpaceFinder that is developed in SenseLess [6]. WhiteSpaceFinder is a database that uses Longley Rice model with terrain data along with TV-tower information to predict the availability of white spaces at any location. We consider a single cell coverage area of 16km-radius in Blacksburg region with $100m \times 100m$ resolution. In our work, we assume that SUs can make use of technologies such as Orthogonal Frequency Division Multiple Access (OFDMA) to utilize subchannels in each 6MHz band. We use graph coloring based spectral allocation to assign available channels to SUs according to their GPS locations.

C. Simulation Results for Attacker Model

For demonstration purpose we assume the range of the attacker to be 1 km. This range depends on the method deployed for mounting the attack. A 1 km range allows us to not impose any heavy restrictions on the attacker capabilities.

We use this model to evaluate the impact of the attack. As mentioned in Section II-A, PU interference is the main concern in the problem under consideration. Therefore, the metric we use to study the impact of a spoofing attack is the number of SUs who interfere with PUs in the worst case. From Figure 1, we can observe that as we increase the number of SUs in the network, PU interference becomes more serious. Also, even in a extremely sparse network with only 100 SUs in the 16km-radius BS coverage range, we still observe PU interference.

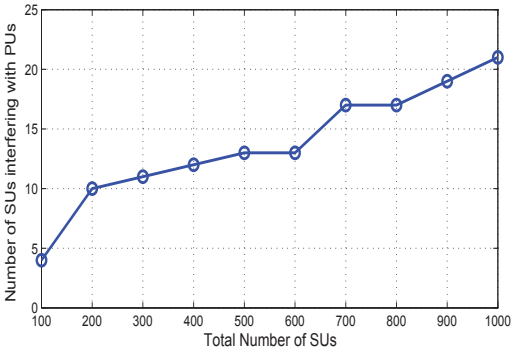

Fig. 1. Variation in severity of PU interference with SU density

We also examine the probability distribution of PU interference among 51 TV channels. Figure 2 shows that most of the PU interference occur on TV channels 35, 38 and 51. This is due to the large variation in the availability of these 3 channels over the whole area. We can say that for a channel whose geographic availability varies a lot, it is more likely that GPS spoofing attack can cause interference.

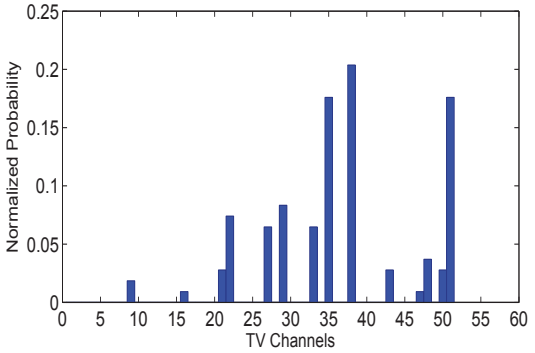

Fig. 2. There are 21 available channels in total. In a 600-SU network, 14 of them are interfered with at least once in 50 simulations.

III. Spoofing Attack Detection

In this section, we propose a distributed location verification method to detect spoofing attacks. We then describe an analytical model and study the efficiency of our detection mechanism.

A. Location Verification Scheme

In order to detect attacks and determine victim SUs in time, BS periodically launches location verification process. At the very beginning, we assume that there are always a certain number of SUs who can hear surrounding WiFi access points. These SUs compare their GPS locations with corresponding WiFi access points' locations prestored in database. If the

comparison shows a match, they assume that their GPS locations are verified[1]. Hence, they become initial anchor nodes. Then, each anchor node transmit a r radius beacon signal containing his position to surrounding SUs with probability β[2]. When an unverified SU hears a beacon signal from any anchor, he checks if his GPS location is within radius r of the anchor's location. If so, that SU trusts his GPS location and becomes a new anchor. Otherwise, the SU will infer that he is under GPS spoofing attack and remain silent. As this location verification propagates through the whole cell, an equilibrium is achieved wherein no further nodes can be verified. The verification process ends at this point. If any SU fails the location verification, BS indicates that the network is under spoofing attack.

Then, the BS needs to identify which SUs are victims and stop allocating spectrum to them. The BS first determines the spoofed location created by attacker through looking at GPS locations of users who failed location verification. BS concludes that all SUs who report the spoofed location are victims and immediately orders them to stop their transmission.

In cases of sparse distribution of SUs, it is possible that spoofed SUs fail to hear any anchor node i.e., they are isolated. In such a case, the BS cannot positively identify whether such SUs are under attack or not. This can lead to missed detection of GPS spoofing attack. We discuss this case further in the evaluation section.

B. Analytical Model

We propose an analytical model for our verification mechanism under no-attack conditions, which is similar to virus spreading model in random geometric networks [7], [8]. We assume that n SUs, $S_n = \{s_1, s_2, ..., s_n\}$, are located at random positions, $L_n = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\}$, where (x_i, y_i) are uniformly distributed in one cell. Each anchor has a beacon range r, which is so-called connectivity radius. We assume two SUs, $s_i, s_j \in S_n$, are connected if and only if $\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq r$. We denote this random geometric graph by $G(L_n; r)$.

Our model uses discrete time. During each time interval, an anchor node transmits a beacon signal with probability β. We denote the probability that a SU i is verified at time t as $p_{i,t}$. We assume that a SU i is verified at time t if

- i was already verified before t.
- i was not verified before t, but receives beacon signals from neighboring anchors and gets verified at t.

Hence, we define the probability of a SU i getting verified at time t to be

$$p_{i,t} = p_{i,t-1} + (1 - p_{i,t-1})(1 - \prod_{j \in Neighbors\ of\ i} (1 - \beta p_{j,t-1})) = 1 - (1 - p_{i,t-1}) \prod_{j \in Neighbors\ of\ i} (1 - \beta p_{j,t-1}) \quad (1)$$

where $i = 1, 2, ..., n$. Given a network topology and specific β value, we can numerically solve equation (1) and obtain time evolution of total number of verified SUs $\mathrm{N}_t = \sum_{i=1}^{n} p_{i,t}$.

We demonstrate that our model performs well by comparing simulation results with numerical results calculated using our model. We set up an initial anchor ratio $\gamma = \frac{Number\ of\ Initial\ Anchors}{Total\ SU\ Number}$ and begin each simulation case with $\gamma \cdot n$ randomly chosen initial anchors. During each time step, anchors attempt to verify neighboring SUs with probability β. Verified SUs simply ignore subsequent beacon signals they receive.

Figure 3 shows the time evolution of N_t predicted by our model and simulation results. As shown, our model yields very good results that match simulation with high accuracy. Our simulation plot averages 30 individual runs and we observe that more individual runs result in better match with our model.

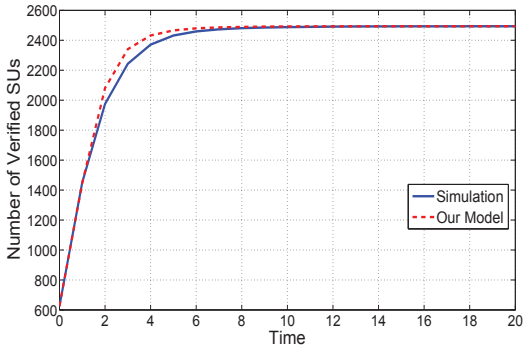

Fig. 3. Time evolution of location verification in a 2500-SU network with $\gamma = 25\%$, $\beta = 0.3$ and $r = 500m$.

C. Spectral Analysis of Convergence Time

The efficiency of spoofing attack detection mechanism highly depends on the convergence time of location verification process. Therefore, we use spectral analysis on our model to find an upper bound of convergence time.
We apply an approximation[3] (2) to equation (1)

$$(1 - \varepsilon)(1 - \mu) = 1 - \varepsilon - \mu, \quad where\ \varepsilon \ll 1, \mu \ll 1 \quad (2)$$

Now,

$$p_{i,t} = p_{i,t-1} + \beta \sum_{j} p_{j,t-1} \quad (3)$$

Using a column vector $\mathbf{P_t} = (p_{1,t}, p_{2,t}, ..., p_{n,t})^T$ to convert equation (3) to matrix form, we have

$$\mathbf{P_t} = (\mathbf{I} + \beta\mathbf{A})\mathbf{P_{t-1}} = \mathbf{B}\mathbf{P_{t-1}} = \mathbf{B}^t\mathbf{P}_0 \quad (4)$$

where $\mathbf{B} = (\mathbf{I} + \beta\mathbf{A})$ and $\mathbf{A}$ is the adjacency matrix of G. $\mathbf{V}_{i,A}$ is the eigenvector of $\mathbf{A}$ corresponding to eigenvalue $\lambda_{i,A}$. By definition, we have $\mathbf{A}\mathbf{V}_{i,A} = \lambda_{i,A}\mathbf{V}_{i,A}$, so

$$\mathbf{B}\mathbf{V}_{i,A} = (\mathbf{I} + \beta\mathbf{A})\mathbf{V}_{i,A} = \mathbf{V}_{i,A} + \beta\lambda_{i,A}\mathbf{V}_{i,A} = (1 + \beta\lambda_{i,A})\mathbf{V}_{i,A}$$

[1] Required localization accuracy for a SU is about 800 m while WiFi access points' transmission range is less than 150 m. Instead of using WiFi signals to precisely localize SUs, we only need to confirm that the GPS locations are within the transmission range of specific WiFi access points.

[2] Anchors transmit beacons in this way to avoid collisions among neighboring anchors. Randomized schemes have proven extremely effective to avoid contentions but we do not study it in this paper.

[3] In our model, it requires a relatively small β to apply this approximation.

Hence, $\mathbf{V}_{i,A}$ is also the eigenvector of $\mathbf{B}$ but corresponding to eigenvalue $\lambda_{i,B} = 1 + \beta\lambda_{i,A}$. Using spectral decomposition on real symmetric matrix $\mathbf{B}$, we have

$$\mathbf{B}^t = \sum_i {\lambda^t}_{i,B} \mathbf{V}_{i,B} {\mathbf{V}_{i,B}}^T \tag{5}$$

Sorting the eigenvalues in non-increasing order such that $\lambda_{1,A} \geq \lambda_{2,A} \geq ... \geq \lambda_{n,A}$ and $\lambda_{1,B} \geq \lambda_{2,B} \geq ... \geq \lambda_{n,B}$. Substituting equation (5) into equation (4), we have

$$\mathbf{P_t} = \sum_i {\lambda^t}_{i,B} \mathbf{V}_{i,B} {\mathbf{V}_{i,B}}^T \mathbf{P}_0 = \sum_i {\lambda^t}_{i,B} \mathbf{C_i} \tag{6}$$

where $\mathbf{C}_i$ are constant column vectors. Thus, time evolution of total number of verified SUs

$$\mathrm{N}_t = \sum_{i=1}^{n} p_{i,t} = \sum_{i=1}^{n} ({\lambda^t}_{i,B} \sum_{j=1}^{n} c_{ij})$$

where c_{ij} is the jth element of constant matrix $\mathbf{C}_i$. Furthermore, we can say

$$\mathrm{N}_t > {\lambda^t}_{1,B} \sum_{j=1}^{n} c_{1j} \Rightarrow t < \log_{(1+\beta\lambda_{1,A})} \frac{N_t}{\sum_{j=1}^{n} c_{1j}} \tag{7}$$

In equation (7), we see that the upper bound of convergence time is a log function with base $1 + \beta\lambda_{1,A}$. Figure 4 plots time evolution of verified SUs and the exponential function ${\lambda^t}_{1,B} \sum_{j=1}^{n} c_{1j}$ in logarithmic scale. We can see that the convergence time is bounded by what indicates in equation (7).

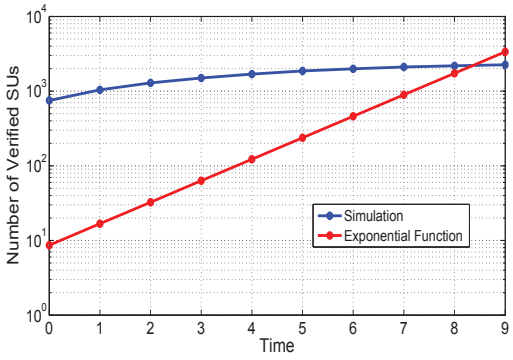

Fig. 4. Simulation results are averaged over 30 individual runs in a 2500-SU network with $\gamma = 30\%$, $\beta = 0.08$ and $r = 500m$.

IV. Evaluation of GPS Spoofing Attack Detection

In this section, we evaluate the detection accuracy of our proposed GPS spoofing attack detection.

According to our detection mechanism, there will be no false alarms under normal situations. So we calculate detection accuracy in the presence of an attacker by launching 100 spoofing attacks. To be conservative, we only assume that the initial anchor ratio $\gamma = 5\%$. In Figure 5, we vary beacon range r and total number of SUs n to grasp the performance under different scenarios.

As seen from the figure, we can achieve nearly 100% detection accuracy with a beacon range $r = 500m$ if total number of SUs $n \geq 800$. We also see that as the SU density increases, high detection accuracy can be achieved

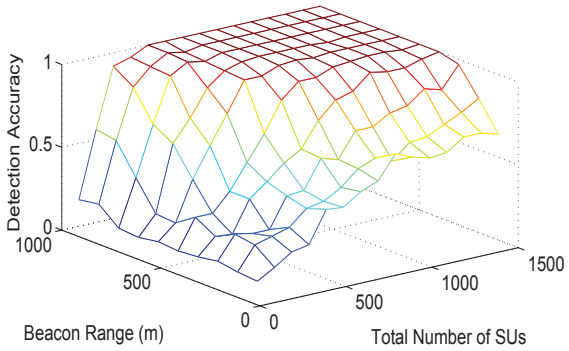

Fig. 5. Impact of SU density and beacon range on detection accuracy with $\gamma = 5\%$

with a relatively small beacon range. For example, using $300m$ beacon range to detect spoofing attack in a 1500-SU network results in nearly 100% accurate detection. Therefore, we can adjust beacon range according to SU density, like a low beacon range for urban area and a higher beacon range for suburb area.

Our detection mechanism requires a certain minimum SU density to propagate which causes an intrinsic limitation. We are not able to handle extremely sparse SU situations. However, attackers are less likely to launch a GPS attack on a sparse network. The reason is that such an attack can hardly spoof enough SUs to cause PU interference in limited trials. Hence, we conclude that our detection mechanism works well for relatively dense SU situations which are very likely for such a large cell.

V. Conclusion

In this paper, we study the impact of GPS spoofing attack on a database-driven WSN and propose a location verification mechanism to detect such an attack. We also present a mathematical model for our detection mechanism and analyze the convergence time of our model.

References

[1] J. Volpe, "Vulnerability assessment of the transportation infrastructure relying on the global positioning system," 2001.

[2] E. L. Key, "Techniques to counter gps spoofing," *Internal Memorandum, MITRE Corporation*, 1995.

[3] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner Jr, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the ION GNSS International Technical Meeting of the Satellite Division*, 2008.

[4] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (gps) is vulnerable to spoofing," *Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[5] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[6] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven white spaces network," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 2, pp. 189–203, 2012.

[7] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos, "Epidemic spreading in real networks: An eigenvalue viewpoint," in *Reliable Distributed Systems, 2003. Proceedings. 22nd International Symposium on*. IEEE, 2003, pp. 25–34.

[8] V. M. Preciado and A. Jadbabaie, "Spectral analysis of virus spreading in random geometric networks," in *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*. IEEE, 2009, pp. 4802–4807.