Virginia Commonwealth University
VCU Scholars Compass

Theses and Dissertations | Graduate School

2013

Exploiting Rogue Signals to Attack Trust-based Cooperative Spectrum Sensing in Cognitive Radio Networks

David Jackson
Virginia Commonwealth University

Follow this and additional works at: https://scholarscompass.vcu.edu/etd

 Part of the Computer Sciences Commons

© The Author

Downloaded from
https://scholarscompass.vcu.edu/etd/3072

This Thesis is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.

www.manaraa.com

©David Jackson, 2013

All Rights Reserved

www.manaraa.com

EXPLOITING ROGUE SIGNALS TO ATTACK TRUST-BASED COOPERATIVE SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at Virginia Commonwealth University.

by

David Jackson
Bachelor of Science in Computer Science
Virginia Commonwealth University, May 2011

Director: Wanyu Zang, Ph.D.
Assistant Professor, Department of Computer Science

Virginia Commonwealth University
Richmond, Virginia
April 2013

www.manaraa.com

ACKNOWLEDGEMENT

A special thank you to my family for their love, support, and forbearance throughout my seven long years of attending Virginia Commonwealth University.

I would like to express my deepest appreciation to my advisor, Dr. Wanyu Zang, who has patiently guided me through the field of cyber-security. She has been very positive and helpful in my transition to a research oriented environment, and her uplifting attitude and kindness have made her a pleasure to work with. I also want to thank Dr. Meng Yu for co-advising me and supporting me in my classes and research. Both Dr. Zang and Dr. Yu have been inspiring mentors, and I look forward to learning more from them in the years to follow.

I am especially grateful to Dr. Krzysztof Cios for having the most influence in my decision to attend graduate school. Without his encouragement, I would have never entertained the idea of higher education or the possibility of becoming a Ph.D. student. I would also like to thank two esteemed colleagues of mine, Tyler Malkus and Ellen Korcovelos, for helping me to revise the writing and presentation of my thesis. Finally, I would like to thank everyone in the Computer Science department, the faculty and fellow students, for making my time here very enjoyable and deeply fulfilling.

www.manaraa.com

Contents

www.manaraa.com

www.manaraa.com

List of Figures

www.manaraa.com

www.manaraa.com

Nomenclature

H_0	Null Hypothesis: absence of primary signal
H_1	Alternative Hypothesis: existence of primary signal
ASIC	Application-Specific Integrated-Circuit
CPE	Customer Premise Equipment
CR	Cognitive Radios
DoS	Denial of Service
DSA	Dynamic Spectrum Access
FC	Fusion Center
FCC	Federal Communications Commission
GD	Global Decision
IEEE	Institute of Electrical and Electronics Engineers
PU	Primary User
PUE	Primary User Emulation

www.manaraa.com

RCD	RSF Clustering Defense
RSF	Rogue Signal Framing
RSS	Received Signal Strength
SSDF	Spectrum Sensing Data Falsification
SU	Secondary User
WRAN	Wireless Regional Area Network

www.manaraa.com

ABSTRACT

EXPLOITING ROGUE SIGNALS TO ATTACK TRUST-BASED COOPERATIVE SPECTRUM SENSING IN COGNITIVE RADIO NETWORKS

By David Jackson

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science at Virginia Commonwealth University.

Virginia Commonwealth University, 2013.

Major Director: Wanyu Zang, Ph.D.

Assistant Professor, Department of Computer Science

Cognitive radios are currently presented as the solution to the ever-increasing spectrum shortage problem. However, their increased capabilities over traditional radios introduce a new dimension of security threats. Cooperative Spectrum Sensing (CSS) has been proposed as a means to protect cognitive radio networks from the well known security threats: Primary User Emulation (PUE) and Spectrum Sensing Data Falsification (SSDF).

I demonstrate a new threat to trust-based CSS protocols, called the *Rogue Signal Framing* (RSF) intrusion. Rogue signals can be exploited to create the illusion of malicious sensors which leads to the framing of innocent sensors and consequently, their removal from the shared spectrum sensing. Ultimately, with fewer sensors working together, the spectrum sensing is less robust for making correct spectrum access decisions. The simulation experiments illustrate the impact of RSF intrusions which, in severe cases, shows roughly 40% of sensors removed. To mitigate the RSF intrusion's damage to the network's trust, I introduce a new defense based on community detection from analyzing the network's Received Signal Strength (RSS) diversity. Tests show a 95% damage reduction in terms of removed sensors from the shared spectrum sensing, thus retaining the benefits of CSS protocols.

www.manaraa.com

Chapter 1

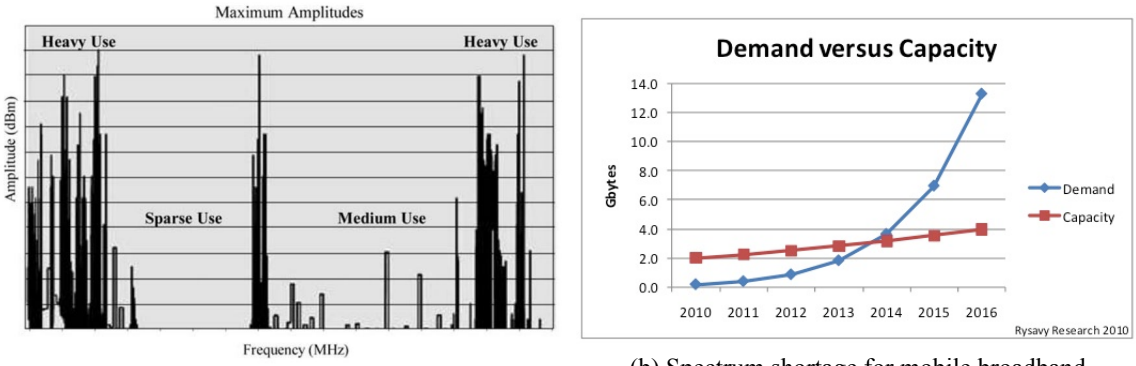
Introduction

This chapter covers the background of my research in the area of cognitive radio networks and their security. Included are the topics of dynamic spectrum access, cooperative spectrum sensing, as well as the common attacks against cognitive radio networks for comparison. Lastly, the section outlines my contributions.

1.1 Cognitive Radios

Cognitive Radios (CR) are adaptive radios that are designed for improved performance and flexibility in wireless communications over the traditional radios that are built upon the more rigid Application-Specific Integrated-Circuit (ASIC) devices. Unlike their predecessors, cognitive radios can be programmed to have any of the following qualities: awareness of their operating environment and their own capabilities, autonomous operations to achieve the radio's goal, and the ability to learn and adapt from past experiences [1]. Their most distinguishing feature is autonomous frequency agility, the ability to change channels dynamically over a broad range of radio-frequency electromagnetic spectrum without the need of user interaction. In contrast, traditional radios broadcast on a single, fixed fre-

www.manaraa.com



(a) Inefficient allocation of spectrum bands

(b) Spectrum shortage for mobile broadband

Figure 1.1: The spectrum shortage problem depicted

quency channel such as the AM/FM radio stations, television networks, cell phones, and so on. In these examples, both the broadcaster and listener have to be tuned to the same frequency to receive a particular service such as music from an FM radio station.

In recent years, the growing demand for wireless services shows an inevitable overcrowding of the spectrum bands, in large part due to the rapid increase of wireless mobile services. The Federal Communications Commission (FCC) has assigned spectrum bands to licensed users for exclusive use on a long term basis, precluding anyone else from access [2]. Yet, analysis of the spectrum bands clearly indicate that current FCC policies have created severely under-utilized spectrum bands (i.e. unused wireless channels), causing a bottleneck for new wireless services. Fig. 1.1a [2] depicts these under-utilized spectrum bands across the usable radio-frequency spectrum. Fig. 1.1b [3] depicts an example of the spectrum demand for mobile broadband services surpassing the available spectrum as early as mid-2013. This example illustrates the need for innovative solutions to alter the trajectory of overcrowded spectrum bands. Dynamic Spectrum Access (DSA) is the proposed solution to alleviate the overcrowding of bands by allowing licensed users, also known as primary-users (PUs), to share unused spectrum with non-licensed secondary-users (SUs) in an opportunistic fashion [2, 4]. An example of a primary network consists of a TV broadcasting station (i.e. the primary transmitter) and the corresponding subscribed viewers (i.e. the primary receivers) [5, 4].

www.manaraa.com

Cognitive Radios are the devices that enable DSA due to their ability to scan spectrum bands and locate the best available channels on a non-interference basis [6]. The exact definition of cognitive radios has evolved and branched off into different meanings. The FCC defines cognitive radios as "a radio system whose parameters are based on information in the environment external to the radio system." [7] The National Telecommunications and Information Agency (NTIA) has proposed cognitive radios to be defined as "a radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operations, such as maximize throughput, mitigate interference, facilitate interoperability, and access secondary markets." [7] However, Joseph Mitola was the first to coin the term "Cognitive Radios" in 1999 and explained it as an intelligent agent that could search out ways to deliver services and adapt the network protocol stack to better satisfy the user's needs [8]. The key aspects associated with Mitola's vision of cognitive radios is that they are [7]:

- **Aware** of surrounding environmental conditions (e.g. the interference for some channel) and the radio's internal state such as the operational parameters for some wireless service;
- **Adapting** to its environment in real time (e.g. switching to a less noisy channel) to satisfy the requirements of some wireless service (e.g. message integrity or Quality-of-Service);
- **Reasoning** on observations to make the best known decisions, which include how to adapt to a particular scenario;
- **Learning** from previous experience to improve its reasoning capabilities; and
- **Collaborating** with other devices to make decisions based on collective observations and knowledge.

These key features require the implementation of artificial intelligence algorithms as an integral part of the CR. However, the research community remains divided on how many, and the scope of, these

www.manaraa.com

features a radio must possess before it is considered a CR. The first large scale standard for cognitive radios, the IEEE 802.22, is primarily focused on frequency agility that addresses the mitigation of interference to PUs [7]. Although cognitive radios are associated with frequency agility and DSA, neither of these features alone account for the main intelligent attribute that cognitive radios were initially known for.

Regardless of how cognitive radios are being interpreted, they are being pushed as the means to solve the spectrum shortage problem by utilizing much of the untapped spectrum bands as illustrated in Fig. 1.1a. The secondary network, consisting of cognitive radios, is given permission to coexist in licensed channels under two preconditions mandated by the FCC: (1) giving spectrum priority to licensed users and (2) minimizing interference to licensed users. The faster the SUs can detect the primary signal and vacate the licensed channels, the smaller the interference to the PUs, thus allowing then the secondary signals to collide less frequently with the primary signal. For this reason, the secondary network must achieve accurate spectrum sensing to know exactly when PUs occupy the channel.

1.2 Spectrum Sensing Methods

Energy detection is perhaps the simplest and most common type of spectrum sensing due to its low cost and the fact that it requires no prior knowledge about the signal characteristics of PUs [9]. An energy detector infers the existence of a PU based on the measured Received Signal Strength (RSS), but it cannot distinguish between PUs and SUs on signal strength alone. To overcome this, all SUs must halt transmission simultaneously in order to listen for the primary signal in a process called the *quiet period*.

Signal feature detection is an alternative technique that uses either cyclostationary feature detection or matched filter detection to capture special characteristics of a primary signal. However, relying solely on signal feature detection may not be adequate to authenticate the primary signal. For

www.manaraa.com

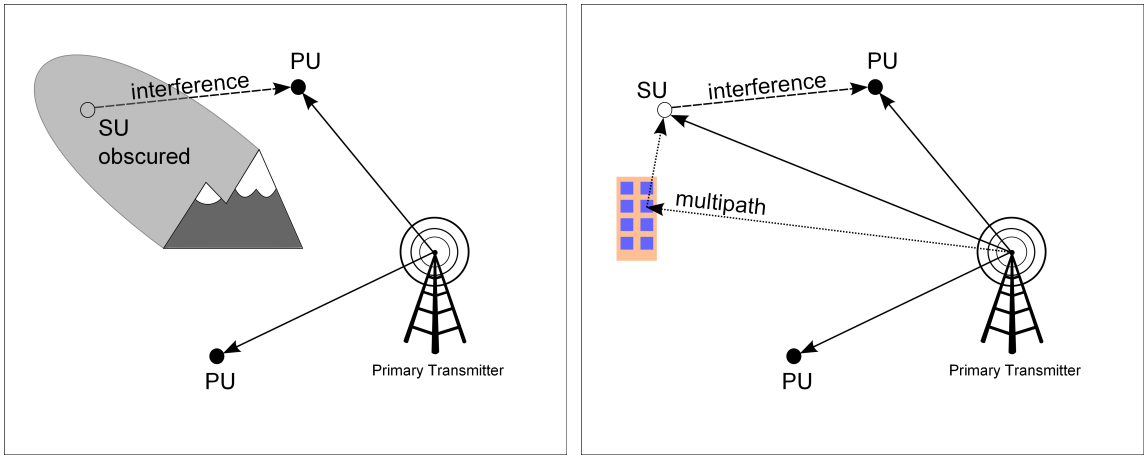
example, in a primary network of subscribed TV viewers, an attacker can transmit previously recorded TV signals that replicate the characteristics of the primary signal [10]. Here, the signal feature detection would fail to differentiate the attacker from the TV broadcasting station. Moreover, conventional replay-attack defenses that require Public Key Infrastructures (PKI) cannot be applied on CR networks, since the FCC mandates require the secondary network to be self-sufficient in detecting the primary signal without any action from the primary network [6]. Hence, key sharing between the primary and secondary networks is not a viable option.

1.3 Cooperative Spectrum Sensing

The cornerstone of the IEEE 802.22 requires the secondary network to surrender channel occupation immediately after detecting the primary signal within the contour region, an area where the primary network is to be protected from interference. Yet, perhaps the biggest obstacle to commercializing cognitive radios is guaranteeing a minimal level of interference to the primary network. This requires that cognitive radios have the ability to reliably detect, in real time, the presence or absence of a primary signal from a given spectrum band. Otherwise, these cognitive radios can unknowingly transmit signals simultaneously with the primary transmitter, causing unacceptable levels of interference to nearby PUs.

Such unintended interference can arise from the hidden node problem. Fig. 1.2a depicts an SU obscured from the primary transmitter due to obstacles in the environment, in what is called shadow fading. Hence, the SU continues to occupy licensed spectrum bands simultaneously with nearby PUs. Additionally, an SU may not detect the primary signal because of multipath fading. This is caused by multipath propagation, the phenomenon that results in a radio signal reaching the receiving antenna in more than one path. In other words, wireless radio signals bounce off physical obstructions, propagating into new signal copies each time, and culminate into a less audible and weaker signal at the receiver. Fig. 1.2b depicts an SU unable to detect the primary signal due to multipath propagation.

www.manaraa.com



(a) Shadow Fading (b) Multipath Fading

Figure 1.2: Causes of the hidden node problem

Research results from [2] indicate that shadow fading and multipath fading can be alleviated by requiring multiple SUs to cooperate with each other to conclude the spectrum availability. This collaboration of sensors, called *Cooperative Spectrum Sensing* (CSS) has been proposed as an effective approach for boosting the detection of primary signals in CR networks [4, 9]. In centralized CSS, the SUs submit their sensor reports to the fusion center (FC), which is a server for aggregating and cross-examining the network's sensor reports for a more robust analysis of the spectrum availability. Here, the FC collects the network's sensor reports and outputs a global decision to notify SUs if they can access a licensed spectrum band. In decentralized CSS, each CR operates as a local FC such that each node makes a local decision on spectrum availability based on its neighbors' data.

1.4 Common Attacks

When a PU is detected on a licensed spectrum band, all SUs must vacate and avoid that spectrum band. In contrast, when an SU is detected, the other SUs may share the channel resources through techniques like Time-Division-Multiple-Access [4]. However, an unauthorized transmission similar

www.manaraa.com

to the primary signal can induce an attack called the Primary User Emulation (PUE) which is when a malicious SU masquerades as a PU in order to monopolize the spectrum resources. For example, a malicious SU can induce a PUE attack by transmitting signals that emulate the characteristics of a TV broadcast station in order to deceive the rest of the secondary network. A successful PUE attack is a false alarm of the primary signal that only affects the secondary network, such that SUs vacate the spectrum band and give the attacker full spectrum access. This can be regarded as a Denial-of-Service (DoS) attack and removes the benefits of DSA.

In contrast, a Spectrum Sensing Data Falsification (SSDF) attack is when malicious SUs intentionally share inaccurate spectrum sensing results in order to change the FC's decision on spectrum availability. Cognitive radios are employed with Software-Defined Radios (SDRs) that supports the operational flexibility required for DSA, which differs from traditional hardware-based radios [4]. This software layer exposes cognitive radios to the threat of malicious software that could manipulate the spectrum sensing results. Unlike a PUE attack, an SSDF attack is not confined by the laws of physics and functions by rewriting the sensor reports at the software layer, such as the RSS values for energy detectors. As such, SSDF attacks have the flexibility to promote the illusion or concealment of the primary signal.

To counter SSDF, various trust models have been proposed to protect CSS [10, 11, 12, 13, 14]. These trust-based solutions build reputations of reporting sensors and filter out sensing reports from those with low reputations. Thus, they can single out attackers and mitigate their influence in the shared spectrum sensing.

1.5 Contributions

I find that the sensor reputations are exploitable by rogue signals in trust-based CSS protocols. In secondary networks, it is very hard to conclude the root cause of bad sensor reports; such as malfunctioning

www.manaraa.com

sensors, the hidden node problem, SSDF attacks, and rogue signals. The trust-based protocols treat all inaccurate sensor reports the same way in that they suffer reputation loss. As a result, attackers can cause inaccurate sensor reports by transmitting narrow rogue signals in order to destroy the reputation of the targeted sensors. Accordingly, I present a new threat to a variety of trust-based CSS protocols, which I name the Rogue Signal Framing (RSF) intrusion. To launch this attack, I exploit directional antennas to isolate a radiation pattern to a group of sensors in close proximity. The outcome is the emulation of an SSDF attack by having rogue signals raise the RSS of a group of sensors much higher than those outside the rogue signal's reach. This contrast leads to innocent sensors being treated as malicious, and consequently removed from the shared spectrum sensing.

To counteract this new threat, I propose a new defense scheme, which I named the RSF Clustering Defense (RCD) module, that looks for dense clusters of sensors from the proximity and similarity of sensor reports in order to look for isolated radiation patterns caused by the RSF intrusion. Thus, the RCD module can distinguish sensors under the RSF intrusion and mitigate the trust damage. I also show that the RCD module is resilient from exploitation by SSDF attack.

The rest of this paper is outlined as follows. Chapter 2 reviews common CR network attacks and trust-based CSS protocols. Then, I present the system model in Chapter 3, and show the details and analysis of the RSF intrusion in Chapter 4. I propose the RCD module, which defends against the RSF intrusion, evaluate its performance in Chapter 5, and conclude the paper in Chapter 6.

www.manaraa.com

Chapter 2

Related Works

My work is mostly related to the following attacks and defenses in CR networks.

While CR networks are vulnerable to a variety of attacks [6], there are two attacks that have received much attention. One such attack is the Primary User Emulation (PUE) [15, 6], where an attacker masquerades as the primary transmitter from the vantage point of its neighbors. The other attack is the Spectrum Sensing Data Falsification (SSDF) [4, 10], in which compromised users falsify the local spectrum sensor reports in order to obscure or create the illusion of the primary signal at the FC [16]. Both attacks affect the FC's perception of the primary signal, ultimately leading to wrong decisions of spectrum accessing. In contrast, the RSF intrusion disrupts the trust between the FC and sensors, which makes the spectrum sensing less stable.

Tom Clancy *et al.* [6] lists a host of threats such as sensory manipulation attacks, belief manipulation attacks, and objective function attacks to cognitive radios with embedded learning engines. However, the RSF intrusion focuses on CR networks with trust schemes and cooperative spectrum sensing, allowing it to work independently of the learning engine.

Bauer *et al.* [24] demonstrates an attack on localization techniques with directional antennas.

www.manaraa.com

The choice of environment for testing the attack was designated for the IEEE 802.11 Wireless Local Area Network (WLAN) environment in an office floor. With the exception of attacking with directional antennas, the RSF intrusion differs in both the environment and objective. In particular, the RSF intrusion is intended for the IEEE 802.22 Wireless Regional Area Network (WRAN) environment and damages sensor reputations instead of corrupting localization techniques.

To defeat the PUE and the SSDF attacks, several trust-based schemes were developed. Chen *et al.* [10] presented a sequential probability ratio test (SPRT) weighted by reputation to mitigate the impact of SSDF attacks. Their algorithm collects sampling votes on the detection or absence of the primary signal, weighing each vote according to the sensor's reputation. For every vote identical to the global decision, the sensor's reputation is incremented, such that their vote carries more weight in future decisions made at the FC. Kaligineedi *et al.* [11] presented a pre-filtering average combination scheme, where the scheme's filters are responsible for (1) removing extreme outlier sensor reports and (2) ignoring sensors that have continuously deviated from the majority over a certain period of time. Arshad *et al.* [13] presented a beta reputation system model for hard-decision CSS protocols. Similar to [10], the sensors are rewarded for agreeing with the global decision, and otherwise penalized. The similarity of these defense approaches is to build reputations for spectrum sensors and thus filter out sensing reports from less trustworthy sensors. However, my work shows that the reputations can be manipulated all too easily, resulting in good sensors being framed and removed from shared spectrum sensing.

www.manaraa.com

Chapter 3

System Model

This chapter discusses the environment used for simulating the Rogue Signal Framing intrusion and its defense. This includes the network layout, the propagation models, the environment's shadow fading, and the attacker's method.

3.1 System Components

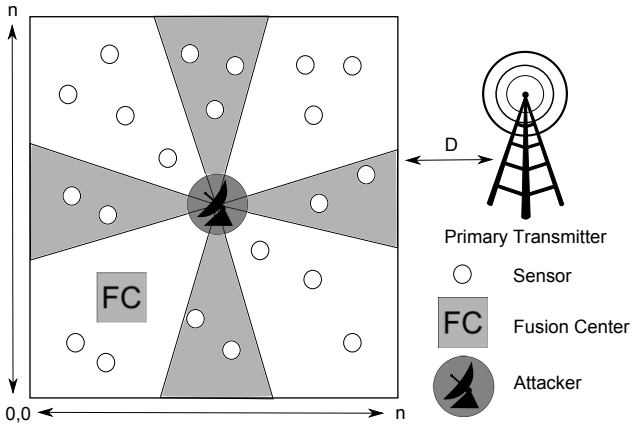


Figure 3.1: Model of Simulation Environment

Without loss of generality, I use a system as shown in Fig. 3.1 to discuss the proposed security

www.manaraa.com

issues. Within the network area, the sensors s_i are randomly distributed and the attacking antennas are positioned at the center. The sensor devices are built in the cognitive radios and operated by the SUs. Spectrum sensing occurs in scheduled time intervals where all SU communications halt, i.e. the *quiet periods*, so that the SU network can listen for the primary signal. The *fusion center* FC then collects the sensor reports and cross-examines them to make a *global decision* GD on the availability of some channel f_0. The GD is a binary hypothesis made after each quiet period that either concludes the absence (H_0) or existence (H_1) of the primary signal. *Energy detection* is the designated spectrum sensing method, so the sensors are only capable of measuring the RSS locally. However, depending on the CSS protocol, the sensor reports may only share the local decision (i.e. H_0 or H_1) instead of the RSS measurement. I assume the sensors are Customer Premise Equipment (CPE) such that their positions are fixed and operate within the households of consumers, and thus forms a static network of sensors, coinciding with the first official standard, the IEEE 802.22, for a wireless regional area network of CPE cognitive radios that have secondary access to the TV frequency spectrum [5].

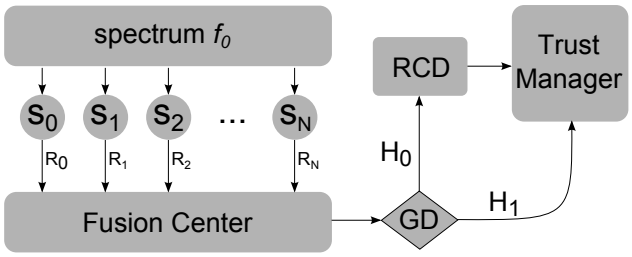


Figure 3.2: Model of Cooperative Spectrum Sensing

Fig. 3.2 shows the flow diagram of operations in my cooperative spectrum sensing model. When a quiet period starts, the SU sensors listen on channel f_0 for the primary signal. Afterward, the SUs deliver their sensor reports to the FC for concluding the spectrum availability and broadcasting the GD to the secondary network. For trust-based CSS protocols, the final step includes storing and updating the sensor trust scores based on the similarity of the sensor reports with the GD, which happens in the *trust manager* module. The RCD module in Fig. 3.2 is my proposed solution to protect the trust manager. Later in Chapter 5, I explain the RCD module in full detail.

www.manaraa.com

3.2 Propagation Model

I use the *Free Space* propagation model (watts) to represent the nearby line-of-sight channels of rogue directional antennas [17]:

$$P_{FS}(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2} \tag{3.1}$$

where λ denotes the wavelength (meters), and G_t and G_r the antenna gains of the transmitter and receiver, respectively. I use the stochastic Rayleigh model to portray a more realistic simulation of the inherent noisy nature of wireless channels [17]. The stochastic equation for the power flux density (watts) is [18]:

$$P_{ray}(P_{FS}(d)) = P_{FS}(d)\sqrt{r_1^2 + r_2^2} \tag{3.2}$$

where $r_1, r_2 \sim \mathcal{N}(0, 1)$.

The greatest factor to affect the RSS (besides attenuation) is the shadow fading gain. The authors in [19, 20] state that realistic shadow fading is statistically correlated to proximity, such that the shadow fading gain is typically more similar for any two sensors the closer they are to each other.

For a more realistic system model, I generate a shadow fading spatial map that is derived from the convolution technique as presented in [20]. This requires a two-dimensional spatial map $[x, y]$ of shadow fading values, denoted as $L_s[x, y]$, with distribution properties of a zero mean and some standard deviation σ_L, i.e. $L_s[x, y] \sim \mathcal{N}(0, \sigma_L)$.

Each position in $L_s[x, y]$ is correlated with another position on a logarithmic scale based on their proximity, which has been shown to be a sufficient representation of real environments [19, 20]. The normalized logarithmic correlation can be expressed by the function [20]:

www.manaraa.com

$$\alpha(\vec{v}) = \exp\left(-\frac{\|\vec{v}\| \ln 2}{D_{corr}}\right) \tag{3.3}$$

where $\vec{v}$ is the change in position $[\Delta x, \Delta y]$, and D_{corr} is a distance threshold for applying the correlation calculations. Next, each position (x, y) needs to be cross-correlated with all positions by [20]:

$$L_2[x,y] = \sum_{i=1}^{N_x} \sum_{j=1}^{N_y} L[i,j]\alpha([x-i, y-j]) \tag{3.4}$$

where $[x, y]$ is the current position being correlated with all other positions $[i, j]$ from Eq. 3.3. The equation is repeated until x and y iterate through the discrete ranges $1 \leq x \leq N_x$ and $1 \leq y \leq N_y$ where $N_x \times N_y$ is the map's resolution. However, equation (3.4) distorts the shadow fading map's distribution, which conflicts with the requirement of having $L_s[x,y] \sim \mathcal{N}(0, \sigma_L)$. This can be corrected by applying the following equation to the entire shadow fading map [20]:

$$L_s[x,y] = (L_2[x,y] - \mu_{L_2})\frac{\sigma_L}{\sigma_{L_2}} \tag{3.5}$$

where μ_{L_2} and σ_{L_2} are L_2's mean and variance, respectively. Fig. 3.3 shows my shadow fading spatial map $L_s[x,y]$ as a 3D mesh that was generated by Eq. 3.5.

The RSS R_i for any given sensor s_i is generated by [21]:

$$R_i = \begin{cases} \mathcal{N}(\mu_\omega, \sigma_\omega), & H_0 \\ 10\log_{10}(P_{ray}(P_{FS}(d_{ij}))) + L_s[x_i, y_i], & H_1 \end{cases} \tag{3.6}$$

where d_{ij} is the distance between the i^{th} sensor and the j^{th} rogue antenna, μ_ω is the noise power mean, and σ_ω is the noise variance. The null hypothesis H_0 is the conjecture of the primary signal's

www.manaraa.com

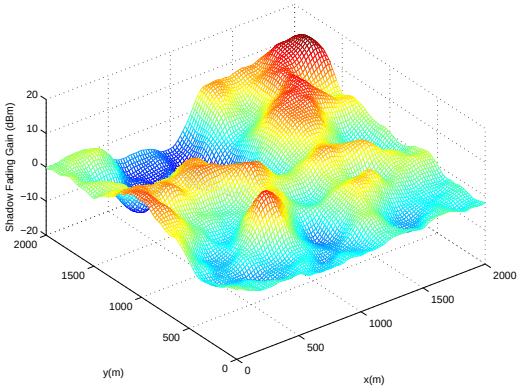


Figure 3.3: A simulated shadow fading spatial map, from Eq. 3.5

absence. The alternative hypothesis H_1 is the conjecture of the primary signal's presence. I assume that the channel bandwidth is much larger than the coherent bandwidth, so the effects of multi-path fading are negligible [5]. Hence, I do not include the multipath fading gain in equation (3.6).

3.3 Directional Antenna Model

My simulations employ directional antennas to transmit rogue signals. The motivation for rogue antennas is explained in Chapter 4. Since the antenna radiates in a smaller area surface, the signal strength is compressed, increasing the power density (i.e. the RSS). The directive gain of an antenna is [22]:

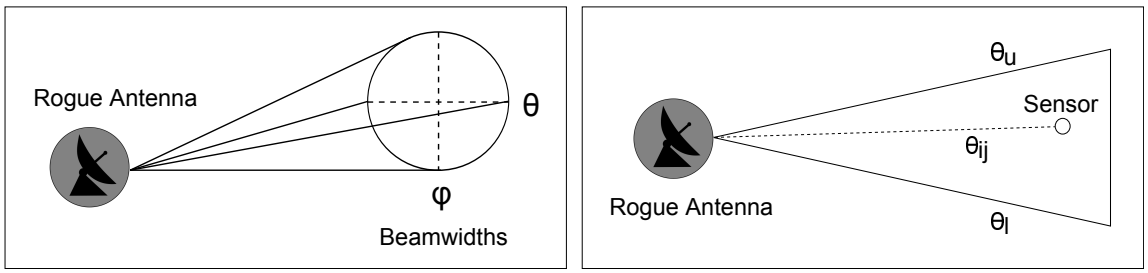
$$G(\theta,\phi) = (4\pi r^2)\left(\frac{4}{\pi r^2 sin(\theta) sin(\phi)}\right) \tag{3.7}$$

where θ and ϕ are the vertical and horizontal angles of the beamwidth, respectively. For simplification, I assume $\theta = \phi$ for equation (3.7). Sensors located outside the area of the radiation pattern are unaffected, which is to say they are out of range of the rogue signal. To determine which sensors are attacked, I need to calculate the angle between the attacked sensor and the directional antenna. The angle between position $\vec{p_i}$ of the i^{th} sensor and position $\vec{p_j}$ of the j^{th} antenna is:

www.manaraa.com

$$\theta_{ij} = \arccos\left(\frac{\vec{p_i} \cdot \vec{p_j}}{\|\vec{p_i}\|\|\vec{p_j}\|}\right) \tag{3.8}$$

where $\vec{p_i}, \vec{p_j} \in \mathbb{R}^2$. The i^{th} sensor can be represented as affected if θ_{ij} falls between the lower and upper beam angles θ_l, θ_u of the j^{th} transmitter such that $\theta_l \leq \theta_{ij} \leq \theta_u$.



(a) Directive Gain (b) Beamwidths

Figure 3.4: Model of Directional Antennas

www.manaraa.com

Chapter 4

Rogue Signal Framing Intrusion

In this chapter, I introduce the Rogue Signal Framing (RSF) intrusion and explain the vulnerability of sensor reputations to rogue signals and the motivation for attacking with directional antennas. Afterward, I demonstrate the impact of the RSF intrusion on sensor reputations through various simulations.

4.1 Security Enforced at the Physical Layer

In the Cooperative Spectrum Sensing paradigm, the spectrum sensors (i.e. the physical layer) provide local signal detection and then reports the results to the FC. Afterward, the FC validates the signal authenticity through cross-examination of the network's sensor reports, as portrayed in Fig. 3.2. For this reason, verifying the source of a signal at the physical layer is incredibly difficult, especially for energy detectors that can only observe the RSS. Authenticating at the physical layer removes the option of cryptographic means to identify the source since it is usually done at the network layer [6]. Furthermore, authentication of the primary signal at higher network layers, e.g. packet headers, is prohibited as a result of restrictions prescribed by the FCC. One restriction in particular states that " *no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum*

www.manaraa.com

by secondary users" [15]. In other words, the primary network is not obligated to assist the secondary network in spectrum sensing, but the secondary network must attest to accurate spectrum sensing so that they do not interfere with the primary network. As such, solutions that involve any interaction between the primary and secondary networks cannot satisfy the FCC's stringent requirements. The motivation behind the separation of communication between the primary and secondary network is to avoid placing additional burdens on the licensed users for the sake of the SUs.

Cognitive radios introduce a new dimension of threats into wireless networks. To achieve highly flexible operating characteristics required for DSA, cognitive radios are implemented as an extension of the Software-Defined Radio (SDR) platform instead of hardware-driven Application-Specific Integrated-Circuit (ASIC) devices seen in conventional radios [4]. From a security standpoint, signal transmission in conventional radio communications is more predictable due to the static allocation of spectrum bands to specific services and the regulation of the manufactured ASIC-based radios.

Sensor reputations and CSS are often used to perform robust and accurate spectrum sensing without having to communicate with the primary network, but the question remains on how effective trust-schemes are at satisfying the FCC requirements. The extended programmability and the operational flexibility of cognitive radios have dramatically increased the attack surface, in that it becomes possible to create a wide range of authorized and unauthorized waveforms with a low-cost consumer devices [23]. In an NSF 2009 workshop, the FCC had raised the question, "What authentication mechanisms are needed to support cooperative cognitive networks? Are reputation-based schemes useful supplements to conventional Public Key Infrastructure (PKI) authentication protocols?" [23] Later in this section, I address certain issues of enforcing reputation-based schemes at the physical layer.

www.manaraa.com

4.2 Trust Vulnerability

CR network protocols must be self-reliant in minimizing interference to the primary network which requires accurate spectrum analysis. In the case of SSDF attacks, trust models have been effective at removing malicious sensors from the shared spectrum sensing [10, 11, 12, 13, 14]. More specifically, sensors are labeled untrustworthy by the trust manager when they have a consistent history of abnormal sensor reports. The trust manager judges each sensor equally, in particular the unreliable sensors without regard to the underlying cause. These causes include malfunctioning sensors, malicious sensors, and sensors affected by the hidden node problem.

Treating all sensors solely based on their reports may at first seem appropriate, but this can also be perceived as an overly sensitive intrusion detection system. Rogue signals can raise a sensor's RSS well above what is expected, especially in the absence of the primary signal. A prolonged rogue signal on the same group of sensors could cause a sharp contrast of sensor reports from the unaffected neighbors, thus appearing malicious and no different than SSDF. Consequently, the security protocol brands these sensors as untrustworthy and removes them from the shared spectrum analysis for as long as the stigma remains. As such, the RSF intrusion constitutes as an exploitation of the trust model. In the context of CSS, I define the term *Rogue Signal Framing* intrusion as follows,

Definition: *Rogue Signal Framing* intrusion breaks the trust between the fusion center and a group of sensors via rogue signals to create the illusion of malicious sensors

To launch this attack, directional antennas are used to isolate a radiation pattern to a group of sensors within proximity, and thereby cause them to report abnormally high RSS values relative to their neighbors who are unaffected by the rogue signal. This scenario emulates an SSDF attack where innocent sensors are perceived as attackers, and consequently removes them from the shared spectrum

www.manaraa.com

sensing. The RSF intrusion should be treated differently than malfunctioning/malicious sensors because the outcome is a long-term consequence. In other words, well-behaved sensors framed by rogue signals are ignored over an extended period of time, even after the rogue antenna stops transmitting. Attackers can leverage the framing of sensors as a stepping-stone attack in order to soften the defense of trust-based CSS protocols for future attacks, such as PUE and SSDF attacks.

The CSS paradigm can be modeled in the context of the Byzantine Fault Tolerance problem. Chen *et al.* [10] described a Byzantine failure as a malfunctioning sensor or an SSDF attack. In both cases, the sensors perform unreliable local spectrum sensing that could ultimately lead the FC to make wrong spectrum decisions like the misdetection and false alarm. A misdetection is when the FC decides H_0 when in fact the primary signal is present, and may result in unacceptable interference to the PUs. Conversely, the false alarm is when the FC decides H_1 when the primary signal is absent, and causes a DoS of spectrum resources for secondary users.

The RSF's ability to damage sensor trust does not directly influence the FC's decision. Instead, the RSF lowers the system's fault tolerance, because the FC has to rely on less sensors to infer the presence of the primary signal. Hence, the RSF weakens the reliability of shared spectrum sensing for trust-based CSS protocols in the aftermath of the intrusion.

4.3 Motivation for Directional Antennas

Isotropic antennas transmit in all directions, maximizing their coverage. In a network of energy detectors, the RSF attacker may need to limit the rogue antenna's coverage in order to avoid a successful PUE, which is an attack on the FC. Directional antennas make it easier to suppress its influence on the FC and frame the targeted sensors, and thus becomes an attack on the trust manager instead. Thus, directional antennas provide a greater degree of control over the isotropic antennas for damaging sensor reputations.

www.manaraa.com

The second advantage is that directional antennas are difficult to localize (i.e. pinpoint) because of their ability to transmit rogue signals with narrow and asymmetrical radiation patterns. Worse yet, the network's RSS diversity is sensitive to any changes to the beam-direction and beamwidth, further complicating the localization. Bauer et. al. [24] empirically tested directional antennas against 802.11 localization algorithms which resulted in very high errors. Isotropic antennas, however, leave massive RSS finger prints in a network of energy detectors due to their wide and uniform radiation pattern. Chen et. al. [15] proposed an RSS-based location verification scheme to detect and pinpoint PUE attacks enforced by a dense network of sensors. However, this scheme was not tested or tailored for pinpointing directional antennas.

4.4 Two Types of Framing

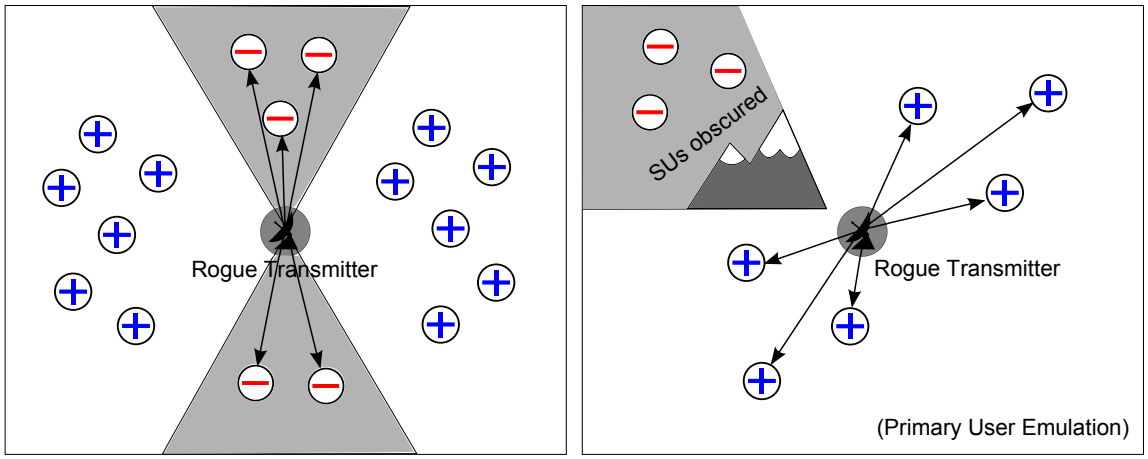
To create an illusion of malicious sensors, there needs to be a separate group of well-behaved sensors to delineate good-from-bad sensor reports. Unfortunately, classifying sensors as either honest or malicious is speculative, as the FCC regulations remove any obligations of the primary network to assist the secondary network [6]. Hence, the secondary network is left to assume channel occupancy (i.e. global decision) with hypotheses like H_0 and H_1. Therefore, if all sensor reputations are in good standing, the global decision is typically determined by the majority of sensors.

This is especially true for hard-decision combining, which is when the FC makes a global decision based on a collection of local decisions, reported by sensors individually, in the form H_0 and H_1. Protocols F_A and F_C use hard-decision combining with sensor reputations. Alternatively, the FC can perform soft-decision combining to determine the global decision based on a collection of non-discrete sensor observations, e.g. energy detectors that report the RSS instead of a local decision.

Soft-decision combining benefits from using more descriptive data, but also becomes more vulnerable to outliers such as in instances where malicious sensors report abnormally high RSS measure-

www.manaraa.com

ments. Generally, CSS protocols are designed to reduce the impact of outliers or remove them entirely, but this still leaves the majority of sensor reports as the determinant of the global decision, just like in hard-decision combining. As such, a majority of sensors will typically decide the global decision, even if that majority is comprised of malicious sensors or affected by a wide-reaching rogue signal, as seen in the case of a PUE attack. In such a case, the FC concludes the disagreeing minority of sensors, even if well-behaved, are presumed inaccurate. Hence, we define two outcomes of rogue signals with regard to damaging sensor reputations, called Type-1 Framing and Type-2 Framing:



(a) Type-1 Framing (b) Type-2 Framing

Figure 4.1: The two outcomes of rogue signals in trust-based CSS protocols

- **Type-1 Framing**: a majority of sensors *not affected by rogue signals* report H_0, so the unaffected minority of sensors report H_1 and appear malicious to the FC, resulting in lower reputation
- **Type-2 Framing**: a majority of sensors *affected by rogue signals* report H_1, so the unaffected minority of sensors report H_0 and appear malicious to the FC, resulting in lower reputation

Prior to this section, Type-1 Framing has been the designated type of trust manipulation to describe the RSF intrusion. Type-2 Framing, which is also a result of rogue signals, is worthy of discussion for simultaneously accomplishing an RSF intrusion and PUE attack. Both attacks are manifested

www.manaraa.com

through radio antennas and can only be distinguished by the attack's outcome, such as misleading the trust manager (via RSF) or the FC (via PUE). Hence, a carefully chosen attack coverage that achieves Type-2 Framing could in fact result in a successful RSF and PUE attack. To my knowledge, the fact that a PUE attack may inadvertently affect sensor reputations has not yet been considered in previous literature. I believe Type-2 Framing is important in that it brings about a greater understanding of PUE attacks against trust-based CSS protocols, which is a very common paradigm of security protocols in CR networks.

4.5 Trust Damage

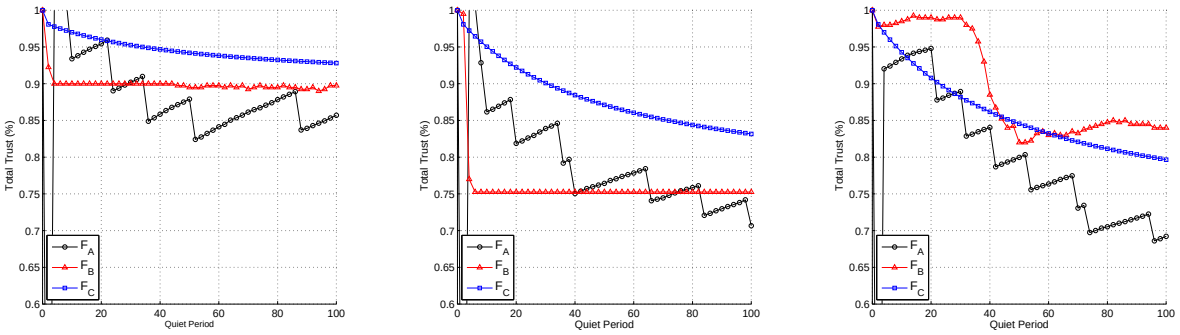
The main goal of the RSF intrusion is to damage the trust between the FC and network sensors. Thus, I use the following equation to measure the network's trust damage $T_\Sigma[q]$ on quiet period q with:

$$T_\Sigma[q] = \frac{1}{T_\Sigma[0]} \sum_{s_i \in S} t_i[q] \tag{4.1}$$

where $t_i[q]$ is the trust score of sensor $s_i \in S$ and $T_\Sigma[0]$ is the initial total trust of the secondary network. For each trust-based CSS protocol, the trust score is represented differently. In order to compare the trust damage between each protocol, I normalize the trust score t_i such that $t_i[q] \in [0, 1]$ in Eq. 4.1.

In each quite period, a group of sensors may lose their trust due to the RSF intrusion, so $T_\Sigma[q]$ changes from one quiet period to the next. As the time passes on, sensors become more susceptible to trust damage under the RSF intrusion, so it is expected $T_\Sigma[q]$ will decrease as the number of quiet periods q increases.

www.manaraa.com



(a) RSF-15 (b) RSF-30 (c) RSF-45

Figure 4.2: RSF Impact - measures trust damage, from Eq. 4.1

4.6 Attack Evaluation of Type-1

To test the RSF intrusion, I borrow three trust-based CSS protocols, mentioned earlier in Chapter 2 and denote them as F_A, F_B, and F_C from [10, 11, 13], respectively.

I make the following assumptions on the simulation's environment according to an IEEE 802.22 WRAN environment that encompasses UHF/VHF TV bands between 54 MHz and 862 MHz [5]. The simulations have 400 sensors located inside a 2000×2000 grid. It is assumed here that the incumbent broadcasting station operates at the UHF frequency of 615 MHz. Like Fig. 3.1, there are four rogue directional antennas facing the cardinal directions and positioned on the map's center. Protocols F_A, F_B, and F_C are tested on three RSF intrusion scenarios, labeled as RSF-15, RSF-30, and RSF-45, and have antenna beamwidths of 15°, 30°, and 45°, respectively. The simulation parameters are listed in Table 4.1.

Fig. 4.2 shows the network's total trust $T_\Sigma[q]$ over 100 quiet periods for each scenario. Depending on the protocol and different evaluation environment, the RSF intrusion removed nearly 15% to 45% of the network's total trust, correlating to the percentage of sensors removed from the shared spectrum sensing. As expected, $T_\Sigma[q]$ decreases, eventually plateauing over time as a result of sensors having no more reputation to possibly lose.

www.manaraa.com

Table 4.1: Simulation Parameters

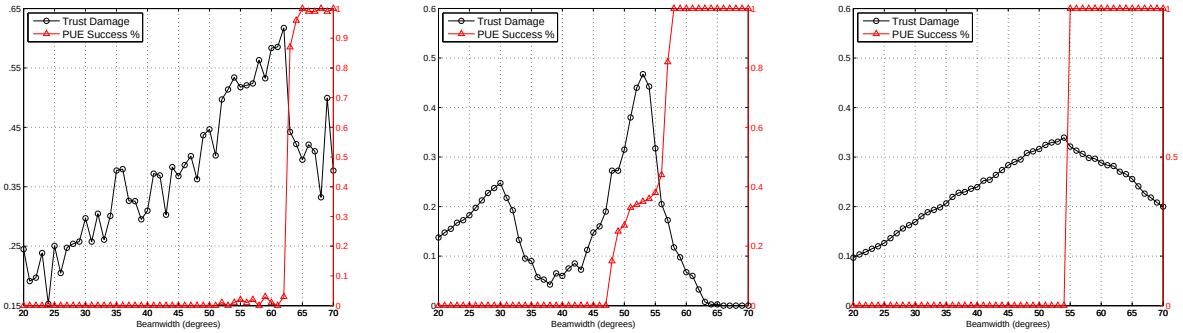
Parameter	Value	Description
N_s	400	Sensors
N_r	4	Rogue antennas
N_x	2000 m	Map length
N_y	2000 m	Map width
γ_θ	-92 dBm	Sensor sensitivity
f_0	615 MHz	Channel frequency
μ_ω	95.2 dBm	Noise power mean
σ_ω	0.3 dB	Noise power std
d_θ	150 m	Distance threshold
σ_L	4.5 dB	Shadow fading variance

In Fig. 4.2, the change in the network's total trust, $\Delta T_\Sigma[q]$, per quiet period is different for protocols F_A, F_B, and F_C, because a sensor's trust score is adjusted differently for each protocol. Hence, these protocols behave differently against rogue signals, but the overall trend is a net loss of total trust $T_\Sigma[q]$ as q increases. I briefly list the general differences in the three protocol designs that led to the unequal outcomes of trust damage:

- **Protocol** F_A: sensor trust is adjusted based on whether its local decision agrees with the FC's global decision; only applies to a random sample of sensors with varying sizes
- **Protocol** F_B: the rate and scope of trust damage depends on the RSS variance because the FC's acceptance threshold of RSS measurements changes with it
- **Protocol** F_C: sensor trust is adjusted based on whether its local decision agrees with the FC's global decision; applies to all sensors

From Fig. 4.2, I observe that both protocols F_A and F_C start to plateau, because the trust t_i of attacked sensors eventually approach 0, causing the $\Delta T_\Sigma[q]$ to become stagnant over time. Conversely, protocol F_B differs in that it does not have local decisions to compare to FC's global decisions. Instead,

www.manaraa.com



(a) Protocol F_A (b) Protocol F_B (c) Protocol F_C

Figure 4.3: Trust damage over 100 quiet periods with respect to beamwidth, and the corresponding PUE success rate

it uses a dynamic threshold for deciding malicious sensor reports which scales with the RSS variance. As the attack coverage increases from RSF-15 to RSF-45, so does the RSS variance and the F_B's behavior towards the RSF intrusion.

4.7 Attack Evaluation of Type-2

Fig 4.1 illustrates two cases of trust damage when the secondary network is bombarded by rogue signals: Type-1 Framing when the minority of sensors are within the attack coverage, and Type-2 Framing when the majority of sensors are within the attack coverage. Assuming the network's trust is in a healthy state, the sensors that disagree with the global decision will be presumed malicious. However in Type-2 Framing, the sensors outside the attack coverage will experience trust penalties.

To show this, I tested for the number of attacked sensors and PUE rate with respect to antenna beamwidth to identify whether trust damage occurs during a PUE attack, or at least from a rogue signal with a wide attack coverage. I followed the same system parameters from Table 4.1. The RSF is launched for a duration of 100 quiet periods with a transmission power of 10 mW for each integral beamwidth, from 10° to 70°. The recorded trust damage is based on Eq. 4.1 with a fixed quiet period

www.manaraa.com

$q = 100$.

The simulation results of Type-2 Framing are depicted in Fig. 4.3 which shows the trust damage $T_{\Sigma}[100]$ and PUE success rate $(\%)$ with respect to antenna beamwidth $\theta°$. Trust damage is evident in all three protocols during successful PUE attacks where the trust damage and PUE success rate are both above 0. In cross examining these results, a negative correlation can be observed between the trust damage and the PUE success rate, especially around the 60° beamwidth mark. Hence, I use these results to reinforce the notion of Type-2 Framing as a result of rogue signals from Fig. 4.1b.

www.manaraa.com

Chapter 5

Rogue Signal Framing Defense

This chapter introductes the RSF Clustering Defense (RCD) module that operates in three steps: 1) analyze the RSS diversity, 2) infer the presence of rogue signals from the first step, and 3) identify and protect the sensors from the rogue signal if detected. The defense relies on the fact that directional antennas leave isolated radiation patterns that form dense communities of sensors. These sensors report the existence of the primary signal, either in the form of a local decision or high RSS measurements. However, malicious sensors can perform SSDF attacks from the software layer without the need of rogue signals, and thus operates outside the physical limitations of signal properties. Therefore, I look toward a solution involving community detection and cluster analysis of the sensor network to identify an RSF intrusion.

5.1 Overview of Networks and Clustering

This section briefly examines the necessary network terms and concepts for better understanding the RCD algorithm and its motivation. I use graph partitioning and community detection as the basis for discovering clusters of RSF-attacked sensors. To partition the graph in a meaningful way, I assume

www.manaraa.com

the nodes (i.e. sensors) have discrete characteristics such as a type or class. In my system model, the sensors are classified based on their local spectrum decision such that a given sensor s_i has a corresponding class c_i where $(c_i = -1)$ if s_i reports H_0 and $(c_i = 1)$ if s_i reports H_1. This allows for the measuring of the network's *assortative mixing*, a term defined as the pairing of nodes with the same class [25]. However, the network of sensors also needs meaningful edges for community detection. The RCD module pairs any two sensors s_i, s_j based on their class c_i, c_j and their mutual distance d_{ij} from each other in order to observe spatial clustering.

The goal of the RCD module is to find an isolated and strongly concentrated group of sensors that report H_1. The Kronecker's Delta Function $\delta(\cdot)$ is a commonly used piecewise constant function in assortative mixing to specify whether or not the two nodes are of the same class [25]:

$$\delta(c_i, c_j) = \begin{cases} 0 & \text{if } c_i \neq c_j \\ 1 & \text{if } c_i = c_j \end{cases} \tag{5.1}$$

A basic mathematical formula for discretely measuring the assortative mixing in a network can be expressed by [25]:

$$\sum_{edge(ij)} \delta(c_i, c_j) = \frac{1}{2} \sum_{ij} A_{ij} \delta(c_i, c_j) \tag{5.2}$$

where c_i, c_j are the node classes and $\delta(c_i, c_j)$ is the Kronecker's delta function from Eq. 5.1. The left side of the Eq. 5.2 is a summation series that iterates through an edge list and increments for each pair of the same class. The right side of Eq. 5.2 is the matrix formula which iterates through an adjacency matrix and increments the same way. The one-half fraction from the matrix formula is there to remove the double counting of pairs.

Consider Fig. 5.1, a network with two classes of nodes such that one class is designated by black

www.manaraa.com

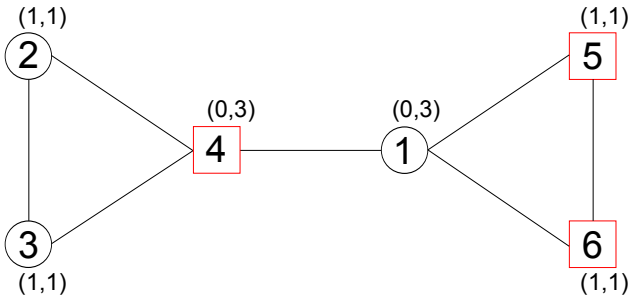


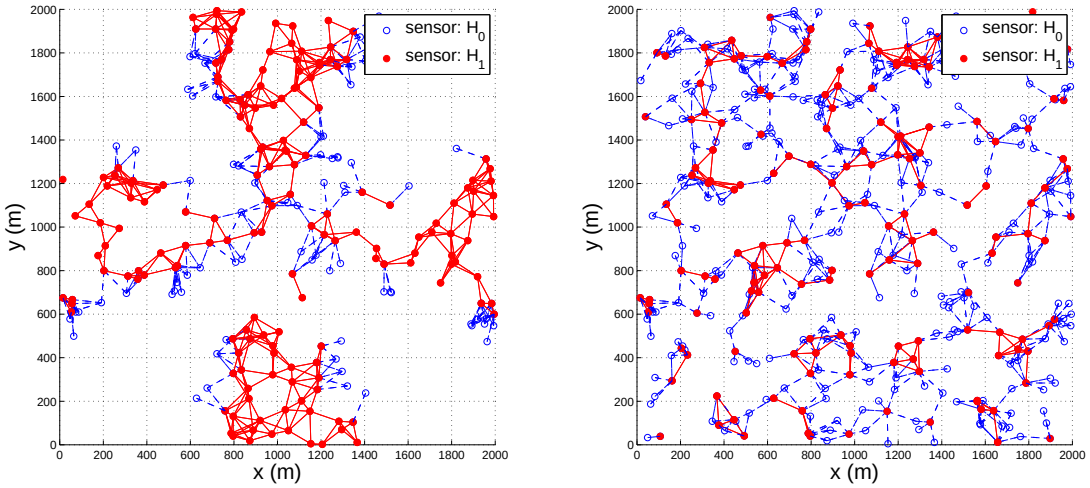
Figure 5.1: Example of assortative mixing

circles and the other by red squares. In such a network, a node can have a degree for each class. Each node n_i keeps track of the number of edges connected to nodes of the same class, denoted as degree k_i^{same}, as well as the number of edges connected to nodes of a different class, denoted as degree k_i^{diff}. The degree k_i^{same} can be computed by Eq. 5.2. Similarly, the degree k_i^{diff} can be computed by the same equation, i.e. Eq. 5.2, with the exception of inverting the sign for the Kronecker's Delta Function. Fig. 5.1 displays these two types of degrees above each node in the form of (k^{same}, k^{diff}) which can be used to measure the strength of the assortative mixing.

5.2 Cluster Analysis Algorithm

My graph partitioning and community detection is based on the principle of assortative mixing, but also has distinct differences. The RCD algorithm generates two graphs, S_{H_1} and S_Δ, out of the sensor network. The graph S_{H_1} pairs sensors s_i and s_j that report H_1 and the distance d_{ij} between them is below some threshold d_θ. The other graph S_Δ pairs sensors s_i and s_j that report differently and are within the same distance threshold d_θ. The result is shown in Fig. 5.2, with S_{H_1} represented as the network with red edges and S_Δ with the blue edges. Afterward, the clustering strength is measured by the difference of degrees from the nodes in S_{H_1} and S_Δ for each disconnected component, which I refer to as the clusters. These clusters are comprised of sensors that share the decision of H_1 and are within distance d_{ij} and remain disconnected from the rest of the network. Each node s_i carries two types of degrees

www.manaraa.com



(a) RSF-45 (b) SSDF-40

Figure 5.2: RCD Clustering - illustrates the clustering method between rogue signals and randomly selected malicious sensors

such that degrees $d_i^{H_1}$ is from the graph S_{H_1} and degrees d_i^{Δ} is from the graph S_{Δ}.

The RCD has three requirements for graph partitioning and cluster analysis. First, it needs the local spectrum decision $c_i \in \{H_0, H_1\}$ for all sensors $s_i \in S$. Second, there must be two sets of sensors where $S_{H_0} = \{s_i | c_i = H_0\}$ and $S_{H_1} = \{s_i | c_i = H_1\}$. Lastly, it needs an adjacency matrix A of size $|S| \times |S|$ such that $A_{ij} = 1$ if the distance $d_{ij} < d_\theta$; else $A_{ij} = 0$, for sensors s_i and s_j, regardless of local decisions.

The RCD module locates k isolated clusters of sensors C_k such that $s_j \in C_k$, $(A_{ij} = 1)$ and $(c_i = c_j)$ for sensors $s_i, s_j \in C_k$. The RCD module's goal is to locate isolated communities of sensors reporting H_1 (i.e. set of C_k clusters) that are distinctly separated by sensors reporting H_0, i.e. sensors in S_{H_0}. To start, I measure the cluster density of sensors with the same class by counting all connected pairs (s_i, s_j) such that $s_i, s_j \in C_k$ and $A_{ij} = 1$. This is computed on all sensors in C_k with:

www.manaraa.com

$$D(C_k) = \{d_i^{H_1}\}_k = \{\sum_{s_j \in C_k} (A_{ij}\delta(c_i, c_j)) - 1 \mid s_i \in C_k\} \tag{5.3}$$

where $\delta(c_i, c_j)$, defined in Eq.5.1, indicates a difference in a node's class c (i.e. the local spectrum decision), $\{d_i^{H_1}\}_k$ is the set of degrees for each s_i such that both s_i and s_j share an edge and report H_1, and $D(C_k)$ is Eq. 5.3 expressed as a function.

Next, I measure the isolation of sensor $s_i \in C_k$ from $s_j \in S_{H_0}$ by counting all connected pairs (s_i, s_j) such that $(A_{ij} = 1)$. This is computed on all sensors in C_k by:

$$D'(C_k, S_{H_0}) = \{d_i^{\Delta}\}_k = \{\sum_{s_j \in S_{H_0}} A_{ij}\delta'(c_i, c_j) \mid s_i \in C_k\} \tag{5.4}$$

$$\delta'(c_i, c_j) = \begin{cases} 0, & \text{if } c_i = c_j \\ 1, & if c_i \neq c_j \end{cases}$$

where $\{d_i^{\Delta}\}_k$ is the set of degrees for each s_i such that both s_i and s_j share an edge and report a different local spectrum decision, and $D'(C_k, S_{H_0})$ is Eq. 5.4 expressed as a function.

Finally, the isolated clustering strength Z_k is measured by:

$$Z_k = Z(\{d_i^{H_1}\}_k, \{d_i^{\Delta}\}_k) = \frac{\sum_i d_i^{H_1}}{\sum_i (d_i^{H_1} + d_i^{\Delta})} \tag{5.5}$$

which is used for deciding the presence of rogue signals. In the off chance that several malicious sensors are positioned near each other, the RCD module uses a specified level of tolerance Z_θ and a required minimum cluster size C_{min} to lower the sensitivity of flagging a rogue signal by mistake. Additionally, C_{min} prevents a high clustering score Z_k resulting from an insignificant sized cluster. The

www.manaraa.com

pseudo-code of the RCD module is displayed in Algorithm 1.

Fig. 5.2 shows two scenarios; the RSF-45 scenario uses the same setup as Fig. 3.1 where each rogue antenna transmits with a beamwidth of 45°, and the SSDF-40 scenario is where 40% of the sensors are randomly selected to become malicious and perform SSDF. The red nodes are sensors reporting H_1 and the blue nodes are sensors reporting H_0. The red edges are formed when $c_i = c_j$ and $d_{ij} < d_\theta$ for sensors s_i and s_j. The blue edges are formed by the same rules except that $c_i \neq c_j$.

Algorithm 1 The RSF Cluster Detection Module

Function:**RCD**(A, S_{H_0}, S_{H_1})

Initialize cluster index $k \leftarrow 0$
Initialize set of protected sensors S_p
Initialize set of visited nodes V
Initialize queue Q
for all $s_i \in S_{H_1}$ **do**
  if $s_i \notin V$ **then**
    $k \leftarrow k + 1$
    Initialize set C_k
    add s_i onto C_k, V, and Q
    while Q is not empty **do**
      $s_q \leftarrow$ dequeue(Q)
      for all $s_j \in S_{H_1}$ **do**
        if $s_j \notin V$ **and** $A_{qj} = 1$ **then**
          add s_j onto C_k, V, and Q
        end if
      end for
    end while
    $\{d_i^{H_1}\}_k \leftarrow D(C_k)$
    $\{d_i^{\Delta}\}_k \leftarrow D'(C_k, S_{H_0})$
    $Z_k \leftarrow Z(\{d_i^{H_1}\}_k, \{d_i^{\Delta}\}_k))$
    if $|C_k| \geq C_{min}$ **and** $Z_k > Z_\theta$ **then**
      $S_p \leftarrow S_p \cup C_k$
    end if
  end if
end for
return S_p

www.manaraa.com

5.3 Resilient to Exploitation

Since I use an environment that conforms to the IEEE 802.22 standard, I assume a static network of CPE sensors. This eliminates the option of malicious SUs moving their sensors closer together in dense clusters with the goal of exploiting the RCD module, such that it protects the reputation of malicious sensors. It is possible that a group of malicious sensors remains in proximity to a static network, by coincidence or otherwise, but the chances of this occurring can be reduced by increasing the minimum cluster threshold C_{min} or the cluster strength threshold Z_{θ}.

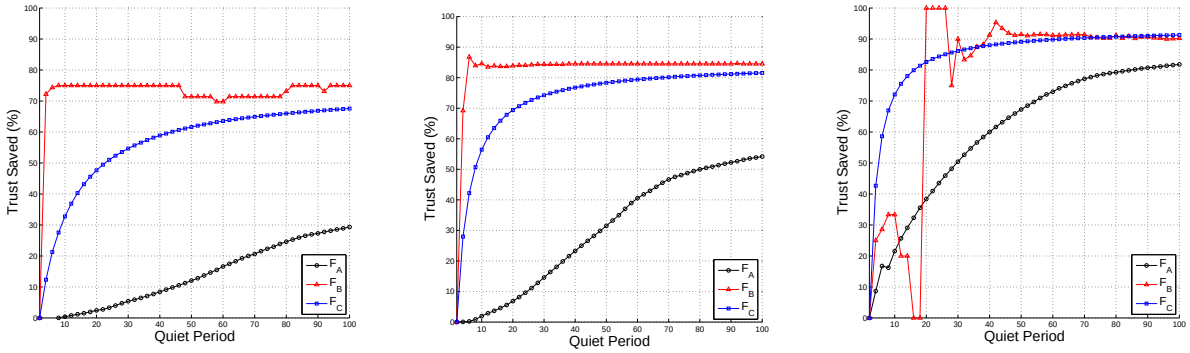
Secondly, the RCD module only functions when the FC decision is H_0 because rogue signals are limited to causing *local* false alarms (i.e. H_1) on attacked sensors. In other words, rogue signals are only capable of switching local spectrum decisions from H_0 to H_1, so the RCD module ignores the scenario of a misdetection. Therefore, malicious sensors attempting misdetection through SSDF attacks will still be penalized when the FC decision is H_1, whether they are clustered or not.

5.4 Defense Evaluation

I have two groups of scenarios, the RSF and SSDF attacks, for the defense simulations. The simulation environment from Chapter 4 is reused for these simulations. The beamwidth of each rogue antenna is 15°, 30°, and 45° for scenarios RSF-15, RSF-30, and RSF-45, respectively. The SSDF scenarios simulate malicious sensors by randomly selecting a percentage of the sensors and raising their RSS by 20 dB from the noise floor. I randomly selected 20%, 30%, and 40% of sensors from the scenarios SSDF-20, SSDF-30, and SSDF-40, respectively.

Fig. 5.3 shows the amount of mitigated trust damage with the RCD module under the same scenarios. I refer to the mitigated trust damage as trust saved $T_S[q]$ and express it with:

www.manaraa.com



(a) RSF-15 (b) RSF-30 (c) RSF-45

Figure 5.3: RCD performance - measures trust saved from Eq. 5.6

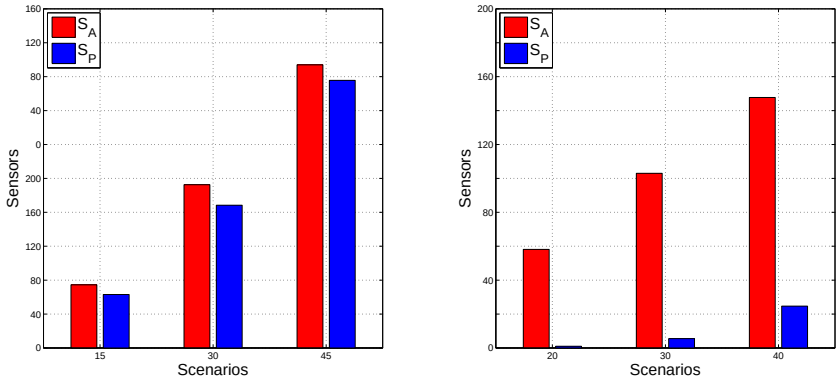
$$T_S[q] = \frac{T_\Sigma^R[q] - T_\Sigma[q]}{T_\Sigma[0] - T_\Sigma[q]} \tag{5.6}$$

where $T_\Sigma^R[q]$ is the network's total trust on quiet period q when using the RCD module, $T_\Sigma[q]$ is the network's total trust without the RCD module (from Fig. 4.2), and $T_\Sigma[0]$ is the initial state of trust scores. I use a minimum cluster size $(C_{min} = 5)$, a clustering threshold $(Z_\theta = 0.3)$, and a distance threshold ($d_\theta = 150$ m).

As shown in Fig. 5.3, each protocol benefited from my proposed defense against the RSF intrusion. However, the RCD module offered less protection to F_A due to its sequential random sampling of sensors, rather than of cross-examining all sensor reports for a more robust analysis. The spikes from F_B in Fig. 5.3 are results of protocol design from having a dynamic threshold for deciding malicious sensors. During the spikes, F_B's dynamic threshold stabilizes as it replaces the old RSS statistics with new data.

Fig. 5.4 compares how RCD module's response to RSF and SSDF attacks in terms of the number of sensors attacked S_A and the number of sensors protected S_P. The goal of my defense is to maximize S_P for the RSF scenarios and minimize it for the SSDF scenarios so that the reputations of malicious

www.manaraa.com



(a) RSF (b) SSDF

Figure 5.4: RCD Sensitivity - counts the number of sensors protected by the RCD module for RSF and SSDF attacks

sensors are not protected. In scenario RSF-45, the strongest RSF intrusion, the RCD module protects 95% of sensors from losing trust. In contrast, the RCD module erroneously protects 15% of the sensors in scenario SSDF-40. This is acceptable as 40% of malicious sensors is an unrealistic and profuse amount of attacks in any CR network. The outcomes of Fig. 5.4 show a high resiliency against the exploitation of SSDF attacks.

www.manaraa.com

Chapter 6

Conclusion

In my thesis, I demonstrated the RSF intrusion, a new threat to trust-based CSS protocols. The attackers can transmit rogue signals onto groups of sensors to emulate SSDF and ruin their reputation with the intent of having them removed from the shared spectrum sensing. My work cautions the use of trust-based CSS protocols and warrants a line of defense against rogue signals. The RSF simulations were conducted in a realistic environment based on the 802.22 WRAN and illustrates the impact of the RSF intrusions on sensor reputation scores. To mitigate the trust damage, I introduced a new defense based on community detection and cluster analysis. The simulation experiments showed that my defense solution, the RCD module, could effectively keep the sensor reputations intact while distinguishing rogue signals from malicious sensors.

www.manaraa.com

Bibliography

[1] Y. Zhao, J. Reed, S. Mao, and K. K. Bae, "Overhead analysis for radio environment mapenabled cognitive radio networks," in *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on*, 2006, pp. 18–25.

[2] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[3] S. Higginbotham, "Spectrum Shortage Will Strike in 2013 — Tech News and Analysis," http://gigaom.com/2010/02/17/analyst-spectrum-shortage-will-strike-in-2013/, 2013, [Online; accessed 08-Apr-2013].

[4] R. Chen, J.-M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 50 –55, april 2008.

[5] S. J. Shellhammer, S. S. N, R. Tandra, and J. Tomcik, "Performance of power detector sensors of dtv signals in ieee 802.22 wrans," in *Proceedings of the first international workshop on Technology and policy for accessing spectrum*, ser. TAPAS '06. New York, NY, USA: ACM, 2006. [Online]. Available: http://doi.acm.org/10.1145/1234388.1234392

www.manaraa.com

[6] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, may 2008, pp. 1 –8.

[7] J. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on*, may 2008, pp. 1 –7.

[8] J. Mitola and J. Maguire, G.Q., "Cognitive radio: making software radios more personal," *Personal Communications, IEEE*, vol. 6, no. 4, pp. 13–18, 1999.

[9] B. Wang and K. Liu, "Advances in cognitive radio networks: A survey," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 5, no. 1, pp. 5 –23, feb. 2011.

[10] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, april 2008, pp. 1876 –1884.

[11] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Communications, 2008. ICC '08. IEEE International Conference on*, may 2008, pp. 3406 –3410.

[12] F. Zhu and S.-W. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," *Communications and Networks, Journal of*, vol. 11, no. 2, pp. 122 –133, april 2009.

[13] K. Arshad and K. Moessner, "Robust collaborative spectrum sensing based on beta reputation system," in *Future Network and Mobile Summit 2011 Conference Proceedings*, 2011.

[14] S. Bhattacharjee, S. Debroy, and M. Chatterjee, "Trust computation through anomaly monitoring in distributed cognitive radio networks," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, sept. 2011, pp. 593 –597.

www.manaraa.com

[15] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on*, sept. 2006, pp. 110 –119.

[16] A. Min, K. Shin, and X. Hu, "Secure cooperative sensing in ieee 802.22 wrans using shadow fading correlation," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 10, pp. 1434 –1447, oct. 2011.

[17] A. Kuntz, F. Schmidt-Eisenlohr, O. Graute, and M. Zitterbart, "Introducing probabilistic radio propagation models in omnet++ mobility framework and cross validation check with ns-2," in *OMNeT++ 2008: Proceedings of the 1st International Workshop on OMNeT++ (hosted by SIMUTools 2008)*. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[18] G. Trenkler, "Statistical distributions: M. evans, n. hastings & b. peacock (1993): (2nd edition). new: John wiley. 170 pages, isbn 0-471-55951,[pound sign] 24.95," *Computational Statistics & Data Analysis*, vol. 19, no. 4, pp. 483–484, 1995. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:csdana:v:19:y:1995:i:4:p:483-484

[19] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electronics Letters*, vol. 27, no. 23, pp. 2145 –2146, nov. 1991.

[20] I. Forkel, M. Schinnenburg, and M. Ang, "Generation of two-dimensional correlated shadowing for mobile radio network simulation," in *Proceedings of The 7th International Symposium on Wireless Personal Multimedia Communications, WPMC 2004*, Abano Terme (Padova), Italy, Sep 2004, p. 5. [Online]. Available: http://www.comnets.rwth-aachen.de

[21] N. Patwari and P. Agrawal, "Effects of correlated shadowing: Connectivity, localization, and rf tomography," in *IPSN*, 2008, pp. 82–93.

www.manaraa.com

[22] A. D. AIR-4.5, *Electronic Warfare and Radar Systems Engineering Handbook*. Washington, DC 20361: Naval Air Systems Command, 1999.

[23] G. M. D. R. Peter Steenkiste, Douglas Sicker, "Future directions in cognitive radio network research," *NSF Workshop*, 2009.

[24] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, "The directional attack on wireless localization -or- how to spoof your location with a tin can," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 30 2009-dec. 4 2009, pp. 1 –6.

[25] M. E. J. Newman, *Networks: An Introduction*. Oxford : Oxford University Press, 2011., 2011.

www.manaraa.com

Vita

David Jackson was born on July 5th, 1988, in Fort Benning, Georgia. He graduated from Brooke Point High School, Stafford, Virginia in 2006. While a college undergraduate student at Virginia Commonwealth University (VCU), he attended three ACM International Collegiate Programming Contests and received two Certificates of Achievement from the University of North Carolina for his performance in 2010 and 2011. In his senior year, he worked in a VCU Biomedical Engineering Lab which resulted in an accepted paper at the ASEE 2011 Conference, titled "Development of Haptic Virtual Reality Gaming Environments for Teaching Nanotechnology". In May of 2011, he received his Bachelor of Science in Computer Science with a minor in Mathematics from VCU. In March of 2013, he won the "Most Innovative App" award at Dominion Enterprises's Hackathon. In April of 2013, he received the "Outstanding Graduate Teacher Assistant Award" by the VCU School of Engineering for that year. After receiving a B.S. in Computer Science, he joined the direct Ph.D. program and became a member of Dr. Zang's security lab.

www.manaraa.com