# Case Study: Security Analysis of a Dynamic Spectrum Access Radio System

**Conference Paper** · January 2011

DOI: 10.1109/GLOCOM.2010.5683726 · Source: IEEE Xplore

T. Charles Clancy
Virginia Polytechnic Institute and State University
**161** PUBLICATIONS **5,220** CITATIONS

Mark McHenry
Shared Spectrum Company
**119** PUBLICATIONS **3,040** CITATIONS

Jeffrey H. Reed
Virginia Polytechnic Institute and State University
**470** PUBLICATIONS **13,296** CITATIONS

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

# Case Study: Security Analysis of a Dynamic Spectrum Access Radio System

Timothy R. Newman [‡], T. Charles. Clancy [†], Mark McHenry [*] and Jeffrey H. Reed [‡]

[†]Electrical and Computer Engineering
University of Maryland, College Park, MD, 20742, USA
[‡]Wireless @ Virginia Tech
Virginia Polytechnic and State Institution, Blacksburg, VA 24073, USA
[*]Shared Spectrum Company
1595 Spring Hill Rd, Suite 110, Vienna, VA 22182, USA

***Abstract*—Dynamic Spectrum Access technology is now well beyond the developmental stages that it was several years ago. Several prototype devices have been created and have been successfully demonstrated at various venues. Recently the FCC has approved the decision for moving ahead with allowing white space devices to operate in the same frequency bands as TV transmitters. Through rigourous testing the FCC has validated the fundamental concept of these DSA radios showing that they can avoid primary users and cause a minimal amount of interference in trusted wireless environments. However, wireless environments can not always be trusted to contain naturally occuring features. Malicious users may introduce false environments such as increased noise levels or emulated primary user signals, in order to fool the DSA device.**

**In this paper, we provide a security analysis on a well established DSA radio developed by Shared Spectrum Company under the DARPA xG program. Our analysis demonstrates the unique security vulnerabilities associated with DSA protocols and expose the extremely low barrier required for a malicious user to exploit them if not security measures are in place. We identify several of these unique vulnerabilities and suggest methods for mitigating them.**

## I. Introduction

Dynamic Spectrum Access (DSA) has been studied and researched vigorously over the past several years, in hopes that it can successfully increase the efficiency that wireless devices access the frequency spectrum. With backing from major research programs at DARPA [1] and legislation at the FCC [2], DSA technology has the momentum to become the foundation for access methodologies of next-generation wireless devices in both military and commercial systems. The majority of research has focused on developing DSA protocols that can guarantee the quality of service of either the primary or secondary users, through specifying key parameters of the DSA algorithm such as probability of detection, signal detection thresholds, or probability of false alarms. However, it is integral to determine how these parameters and the algorithms themselves affect the overall robustness and security of the radios to malicious wireless devices.

The inherent nature of adapting to the environment introduces unique vulnerabilities that have not been encountered by past wireless systems. Recent research has brought up the notion of primary user emulation (PUE) attacks [3], [4], or a malicious user introducing a signal in hopes to cause the DSA radio system to classify it as a primary user and therefore switch channels. In addition to PUE attacks, Denial-of-Service (DoS) attacks on DSA radios have also been briefly studied [5]. However without a simulations or a practical analysis of these threats it's difficult to understand the true impact and develop the mitigation techniques required to alleviate these threats.

In this paper we describe PUE attacks, (DoS) attacks, and spectralhoneypot attacks that are unique to DSA wireless systems. To better understand the practical impact these attacks have on DSA systems, we perform these tests on a real DSA radio system. Developed by Shared Spectrum Company, the DSA 2100 radio is a well tested and mature DSA radio system that well represents the current state of DSA radio technology today. Using these results we conclude with several mitigation techniques designed to increase the robustness of DSA radio to these new and unique threats that the DSA technology itself introduces.

## II. DSA Unique Security Issues

### A. Primary User Emulation

Primary User Emulation (PUE) attacks are DSA radio specific threats whose objective is to present a signal to s DSA enabled secondary user, such that the signal appears similiar enough to a valid primary user's waveform that the DSA enabled secondary user classifies the masquerading signal as a primary user. Recent literature

978-1-4244-5637-6/10/$26.00 ©2010 IEEE

has introduced these attacks [3] and have suggested defensive measures to mitigate PUE threats [4].

PUE attacks are at the front-line of DSA security threats and are typically the foundation and starting point for many more destructive DSA related attacks. Throughout this paper, the attacks that are described all spawn from the ability to emulate a primary user in order to manipulate a radio. In the ideal case, a DSA radio could classify a signal with 100% probability, and be completely robust against false signals attempting to masquerade as a primary user. However in reality this it is not possible to have perfect accuracy. Many obstables prevent current technology from doing this. For example, a malicious user may use the exact waveform of the primary user, especially if the primary user is using a published standard (e.g. IEEE 802.11 or IEEE 802.16). Without additional behavioral information about the waveform, it would be impossible to accurately classify a waveform whom features are exactly the same as the primary user.

### B. *DSA Denial-of-Service*

Denial-of-Service (DoS) attacks have been applied from physical layers all the way to application layers. Most commonly used when referring to a specific type of threat against packet networks, DoS attacks generally imply that the objective of the attack is to disrupt communication or any type of service provided by the targeted node [5].

Dynamic Spectrum Access presents a new set of challenges when it comes to DoS attacks. The ideal vision for DSA technology is to completely mitigate jamming and DoS attacks by having an ultra flexible physical layer that can adapt to the potential threats in the spectrum domain. However, in a practical sense, the flexibility in the physical layer causes second order problems. While it is true, DSA technologies can change frequencies if a jammer is present, the change in frequency comes at a price. It takes a specific amount of time to rendezvous with other nodes in the network, even if a predefined channel has been negotiated before channel adaptation. Tuning the transmitter or receiver to another channel, detecting and coding or uncoding packets, and sending reply packets, are all required to setup communications on a new channel. In DSA enabled radios, it is critical to minimize this time, as it is the cost of adaptation. It is also important to think of the coordination that is done at higher levels whenever multiple radios rendezvous to communication. One specific example is authentication between the communicating parties. Not only do typical authentication protocols require a significant amount of overhead, but each authentication instance if a malicious user knows the location of the signals and the time at which the authentication takes place.

### C. *Spectral Honeypot*

Due to the inherent relocation methodology of DSA protocols, a malicious user now has the ability to guide the DSA radio to a target channel. In the most trivial case this is done by performing a PUE attack, causing the DSA radio to change channels, until the DSA radio lands on the target channel. In essence the malicious user is setting up a spectral honeypot to lure the DSA radio to a specific channel.

There are many reasons why a malicious user may want to force another radio to a specific channel. One reason is to attempt to cause the DSA radio itself to degrade the communication of another system, whether it be another secondary user is operating in the target channel, or the DSA radio has known out-of-band spurs. However, these spurs should be well known by the radio itself which could sense for signals in the channels that the spurs would occupy in an attempt to avoid this. Another reason for performing a honeypot attack is to force a possible man-in-the-middle (MITM) vulnerability. In a general MITM scenario, an attacker wants to position itself in between the transmittor and receiver in order to intercept the signal and possibly insert his own malicious signal. This may be more likely to happen on specific channels, thus a malicious user may need to execute a honeypot attack to guide the DSA radio to this vulnerable channel.

In our analysis we explore the possibility of forcing the radios to a target channel and measure the amount of time is typically takes for this to happen. We look at two different techniques for the spectral honeypot in order to determine if a smarter detect and transmit scheme is better than a simplistic scheme where we sweep the whole band continously. In each technique we stop transmission once the DSA radio lands on the target channel.

## III. Case Study: Shared Spectrum DSA 2100

To explore the security issues prevalent within DSA radio technology, we have decided to use the DSA 2100 radios available from the Shared Spectrum Company [6]. These radios represent the most mature DSA radios currently available. While several other manufacturers and wireless development companies have DSA radios, the majority are in early prototype form and are not available. These radios and the protocols within, represent a major ongoing DSA initiative and we felt also represent the current state of DSA radios as a whole.

The tests were designed to demonstrate basic security vulnerabilities within DSA systems. All the tests we describe below are applicable to generic DSA radios are were not designed specifically for the SSC radios. The tests we perform fall into three different categories:

- Primary User Emulation

- Denial of Service
- Spectral Honeypot Attacks

In order to explore both limits and practical issues related to DSA security, we perform our analysis using two different environments. The first environment is referred to as the High Performance Environment. For this analysis we use the Signal Generator to generate the signals as seen by the DSA radios. Using the signal generator we have generate signals with a high degree of reliability, control, and flexibility in the parameters that are controllable. However, we don't have the intelligent control that is needed to fully explore DSA algorithms in a more practical environment. We refer to this testing environment as the Practical Testing Environment. In this environment we use the Universal Software Radio Peripheral (USRP) [7] connected to a laptop and the GNU Radio software framework as the system platform.

### A. Primary User Emulation Analysis

The DSA 2100 radios were designed for fast and efficient primary user detection A major attribute of the DARPA xG program was to cause "no harm" or no interference. In order to best achieve this goal, a simply and fast primary user detection algorithm was used. To determine whether an observed signal was a primary user, the Shared Spectrum Company radios used the energy of the signal as the primary feature to determine the classification. In order to control this feature, a variable threshold can be configured for a specific wireless environment.

In our analysis and the results shown in the following sections, the energy detection threshold that is used is -105 dBm. This means that if the recieved energy of a signal at the DSA radio is above -105 dBm, anywhere within the operating band 350 MHz to 450 MHz, then at that location, a channel is classified as occupied and is unusable for a specific amount of time. This non-occupancy period is also an extremely important parameter with regard to DSA operation and DSA security vulnerabilities. The purpose of keeping a channel blocked, even though a primary user is not in the channel, comes from the fact that many waveforms are bursty and operate in a single channel in an "on-and-off" manner. Using a non-occupancy period prevents the DSA radio from continuously attempting rejoining a channel where a primary user is using a form of bursty communication. The non-occupancy period is designed to minimize this interference to the PU.

The non-occupancy period poses a unique security tradeoff for DSA radio systems. The potential security risk comes from the fact that the DSA system may unnecessarily lock out channels that may be available and needed in a malicious environment. This non-occupancy period can be abused by malicious users in order to manipulate the DSA radio system. Increasing the non-occupancy period further limits the flexibility of the DSA radio, yet decreases the chance that unnecessary channel adaptations will occur in a bursty communication environment. Thus an important trade-off exists between the non-occupancy period and potential security problems. The following sections demonstrate how the non-occupancy period can be abused to limit throughput and manipulate the behavior of a DSA radio. In the following analysis and results, the non-occupancy period is set to 5 seconds.

### B. Denial-of-Service Analysis

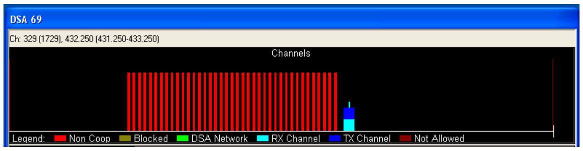
The DoS analysis that we present results of the packet loss due to both simplistic or traditional sweep jamming effects and smart DoS attacks that sense the location of the signal and then send a low power tone to trigger a channel adaptation. The packet loss measurements were performed using the Iperf performance measurement tools [8].

The high performance tests using the signal generator delivered a sweeping pulse over the entire 100 MHz band and varied the dwell time to determine the relationship between loss of throughput and loss of packets versus the amount of time dwelling on the channel. It's important to note that the dwell time is directly related to the amount of time it takes to sweep the complete frequency band of interest. Tests with short dwell times cover the entire band much quicker than tests with larger dwell times.

The non-occupancy period determines the effective block size of the sweeping DoS pulse signal. Figure 1 shows a block of channels that have been deemed unusable because they have recently had a primary user detection. This figure shows a pulse signal at approximately -90 dBm of received power at a dwell rate of 100 ms causing a block of unusable channels to emerge that is 50 MHz wide.

As opposed to the signal generator sweeping pulse, the GNU radio application detects the current operational channel of the DSA radio and sends a pulse just above the current energy threshold to cause the radios to change frequencies. This technique does not waste transmit power sweeping over channels that do not currently have DSA radios operating on them, as it efficiently senses and then transmits a pulse. Figure 2 shows the results of the relatively smarter sense and pulse test as opposed to the transmit only sweeping test.

Figure 2 shows the results of how varying the dwell time of the sweeping pulse signal affects the packet loss between two DSA radios for both the high performance tests and the adaptive tests on the lower quality hardware. It is clear from the figure that between 30 ms to 60 ms of dwell time on the sweeping pulse causes the maximal packet loss. Note that the system never reaches



DSA 69

Ch: 329 (1729), 432.250 (431.250-433.250)

Fig. 1. Channelized spectrum view from the DSA radio perspective showing a block of unusable channels as a result of the non-occupancy period. The small block is the current channel location of the DSA radio operation, while the tall blocks denote unusable channels.

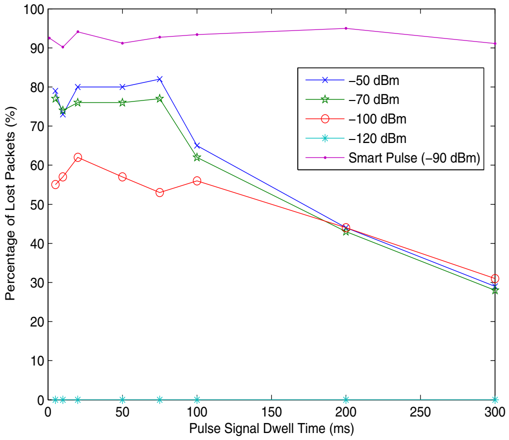
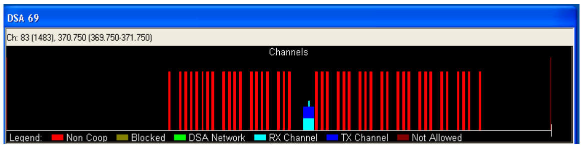


Fig. 2. Packet loss versus the pulse dwell time for sense and pulse DoS test. Results are compared to the high performance pulse sweep tests

completely zero throughput. This indicates that the DSA radio will always introduce a minimal amount of finite interference to the PU during the co-channel sensing and evacuation phase. The packet loss results show that the worst case is approximatly 82% packet loss, and can be lossly generlized to system throughput losses of 82% for the sweeping tests.

The smart pulse line indictates that a malicious user with access to a more adaptive device is able to sustain approximately 92% packet loss. It is clear that even when using the USRP and the GNU radio software framework running on a general purpose processor, it is possible to severely degrade the communications of a DSA radio. These results have nothing to do with the specific implementation of the DSA algorithms themselves by Shared Spectrum Company, and everything to do with the inherent lack of robustness in DSA technology using listen-before-talk (LBT) rule sets. In the end, if the malicious device is able to sense and jam before the DSA network is able to rendezvous it is able to cause the DSA network to become completely unstable.



DSA 69

Ch: 83 (1483), 370.750 (369.750-371.750)

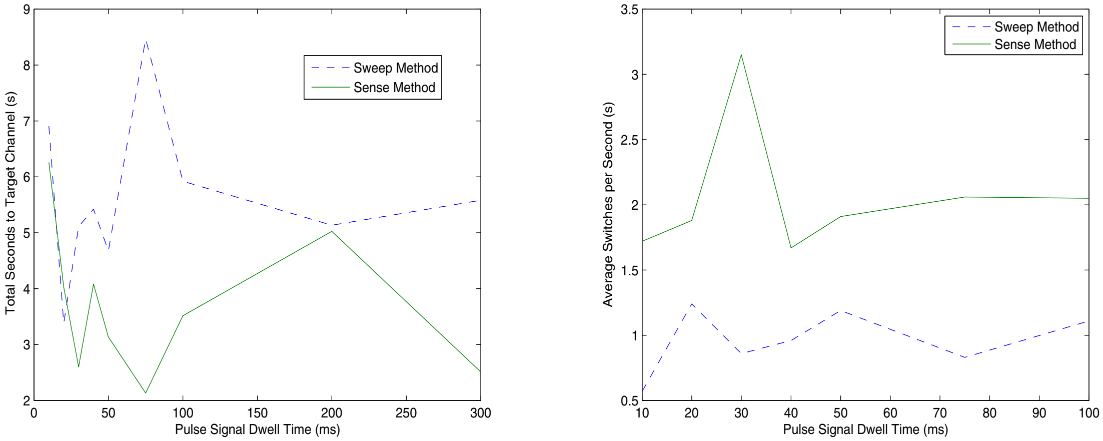
Fig. 3. Channelized spectrum view from the DSA radio perspective showing a block of unusable channels with the target channel carved out and the DSA radio operating inside the target area. The dwell time is set at 60 ms for this test.

### C. *Spectral Honeypot Analysis*

In our spectral honeypot analysis we determine how easily a DSA radio is forced to a target channel. This attack can be performed in a smart manner, by detecting the presence of the DSA radio, and then transmitted a PUE signal to cause adaptation, or it can be done in a more simplistic manner of simply sweeping the band causing adaptation until eventually the DSA radio lands on the target channel. As noted previously the tested configuration uses a lowest energy channel selection mechanism to determine which channel to tune to.

In our high performance tests, the signal generator is restricted to a deterministic and static list of pulses that can be transmitted. To create a target channel, we carve out a chunk of spectrum where the signal generator does NOT transmit. With a carved out chunk of spectrum, the DSA radio will continuously observe this chunk as free. This constant absence of signal on the target channel increases the probability that the radio will decide to operate on the targeted channel.

For each test we started the BS and allowed it to settle on a channel. We then started the signal generator pulse sweep transmission and stopped the signal generator after the BS selected a channel within our targeted 2 MHz band. The time it took for the targetted channel to be reached was determined from the logs on the radio. Figure 3 shows the view from the DSA radio perspective of the channelized spectrum. The figure shows a block of unusable channels surrounding an open section of channels that has been selectively carved out of the sweeping jammers channel list. This result in the DSA radio selecting these channels to operate on because of the average lower amount of energy that is being observed in this section of channels. Figure 4 shows the relationship between the dwell time and the time, in seconds, that it took for the radio to select the targeted channel for both the high performance tests and the practical tests using the USRP and GNUradio. Each data point was averaged over 5 tests. For these tests we targeted a single frequency, 420 MHz. The average time to force the DSA radio to a target channel is 5.6 seconds when using the sweeping method, and 3.7 seconds when using the sense and pulse method. Similar



(a)

(b)

Fig. 4. (a) Dwell time for the pulsed signal sweep versus the time required to force the radio to a target channel. Data is plotted for both the trivial sweep method and the more intelligent sense and pulse method. (b) Average number of channel switches per second versus the pulse dwell time.

to the DoS analysis, the dwell time directly affects the total amount of time it takes to sweep the entire operating frequency band one time. The sense and pulse method took significantly less amount of time to get the DSA radio to the target channel. Varying the dwell time in the sweeping tests create a larger block of unusable channels, giving the DSA radio less opportunities for channel selection. For the sense and pulse method, the dwell time only affects the speed at which the malicious radio causes adaptation in the DSA radio.

Figure 4 (b) shows the average switches per second that each method causes. The dwell time location of the peak was slightly shifted as opposed to the high performance test. This difference is most likely due to the high variation in dwell time associated with running these tests on the practical equipment. Without a real-time operating system using a high level of timing and jitter guarantee, the dwell time for our practical tests may not reflect the same accurate dwell times as the high performance tests. However, the trends in both tests are similar.

The other useful set of data in Figure 4 (b) come from the sense and pulse method. In the sense and pulse method, the average channel switches per second ranged from 1.7 to 3.2. Note that this higher frequency of channel adaptations caused by the sense and pulse method, also contributes to the higher packet loss results that were presented in section III-B. Figure 2 (a) shows the lowest throughput at 30 ms dwell time, which corresponds with the peak of channel switches per second also at 30 ms dwell time. Observations of the channel switches can be done by malicious users to determine the optimal dwell time in order to create the minimal throughput.

## IV. Mitigation Techniques

In this section we discuss several different mitigation approaches that can be applied to mitigate the threats that have been previously discussed.

### *A. Securing the "Frontline"*

Mitigation strategies for DSA vulnerabilities begin at securing the frontlines, or the signal detection and classification stage. In the described vulnerabilities in this paper, each threat has the attribute of using a PUE attack to enable the threat. Without the possibility of a PUE attack, inducing multiple channel adaptations to reduce the quality of service and forcing the operation of the DSA radio to occur on a specific channel is not possible.

Unfortunately it is nearly impossible for signal detection and signal classification techniques to perform perfectly. This is because signals features are not unique and can always be emulated. Whether it be using energy as a signal feature as was demonstrated in this paper, or even using high-order cyclostationary signal analysis to pull out computationally complex and relatively unique signal features, with enough time and computational power all signal features can be emulated. However, this is analogous to encryption and decryption schemes. Given an unlimited amount of time and processing power, even the strongest encryption schemes can be broken, although it may take many lifetimes to do so. It is for this reason that we consider many of these encryption algorithms practically unbreakable.

DSA algorithms, specifically the signal detection and classification techniques must also take the same approach to securing their systems. Creating a robust detection system that is practically unbreakable should be done by using only the most unique signal features that are extremely difficult to emulate. However, a practical tradeoff exists between the computational complexity required to detect and classify a signal using complex signal features and the robustness of the DSA algorithm. In general, in order to guarantee an extremely robust classification system, high performance processing is required because of the intense signal processing that is needed. Many different signal classification systems exist, but the most appropiate, and most robust techniques should be chosen based upon the hardware platform that is used.

### B. Random Non-Occupancy Period

To mitigate the DoS vulnerability caused by non-occupancy periods, visible in Figure 1, while still minimizing overhead in a bursty environment, the DSA algorithm can randomize the non-occupancy period for each change in channel. For example, instead of signalling the channel to be unusable for a constant 5 seconds after a primary user is seen, change this period to a random number of seconds from 1 second to 5 seconds. This will effectively create random holes in the previously described contiguous wideband jamming block, resulting in the DSA radio signal being able to relocate within the block. The proper maximum and minimum values for the non-occupancy period should be determined based upon the communications environment specific to the radio. It may even be possible to completely disregard the blackout period and only tag channels unusable if a primary user is currently transmitting on a channel.

## V. Conclusion

The vulnerabilities orginate from the inherent characteristics of the DSA methodology of reacting to the environment. We have shown in this study that these vulnerabilities can be exploited with only a small amount of energy. Each of the DSA jamming signals was a narrowband tone requiring a small amount of energy. This is much different from the traditional wideband and large power jammers that require significant energy and power. The results have shown how a significantly large number of adaptations requires more system overhead that takes away from the goodput of the system. This overhead is present at all layers of the communications stack, from the signal detection functions to the authentication. Overhead requirements for items such as authentication are typically performed at a higher layer and can require a significant amount of time relative to the total rendezvous time. This motivates the rethinking of where specific overhead sensitive components are implemented in the communications stack for DSA systems. Moving to a more physical layer oriented authentication schemes [9], such as Specific Emitter Identification systems [10], could minimize overhead associated with overhead sensitive components in an extremely dynamic spectral environment.

In conclusion, it is extremely important to validate this environment to the fullest extent possible and design DSA systems such that they are robust to malicious users, yet can still perform the intended operational objective of causing minimal interference to the primary users while at the same time maintaining a communications links for themselves. Unfortunately, as we have shown, developers can and must make certain tradeoffs to achieve the highest priority system design requirements. As this technology progresses, signal classification algorithms and the hardware platforms that these technologies are deployed on also must progress in order to keep these future technologies secure.

## References

[1] DARPA, “The next generation program.” http://www.darpa.mil/sto/smallunitops/xg.html.

[2] FCC, “FCC adopts rules for unlicensed use of television white spaces.” http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-286566A1.pdf.

[3] R. Chen and J. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” in *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, pp. 110–119, September 2006.

[4] R. Chen, J. Park, and J. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, January 2008.

[5] G. Jakimoski and K. Subbalakshmi, “Denial-of-service attacks on dynamic spectrum access networks,” in *IEEE International Conference on Communications Workshops*, pp. 524–528, May 2008.

[6] Shared Spectrum, “Shared spectrum company website.” http://www.sharedspectrum.com.

[7] M. Ettus, “Building software radio systems: The usrp product family,” http://www.ettus.com/downloads/er_broch_trifold_v5b.pdf.

[8] “Iperf performance measurement tool.” http://sourceforge.net/projects/iperf/.

[9] J. B. P. Yu and B. Sadler, “Physical-layer authentication,” *IEEE Transactions on Information Forensics and Security*, vol. 3, pp. 38–51, March 2008.

[10] K. Kim, C. Spooner, I. Akbar, and J. Reed, “Specific emitter identification for cognitive radio with application to ieee 802.11,” in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pp. 1–5, 30 2008-Dec. 4 2008.