Security in Dynamic Spectrum Access Systems: A Survey

Saman T. Zargar, *Member, IEEE*, Martin B. H. Weiss, Carlos E. Caicedo, *Member, IEEE* , and James B. D. Joshi, *Member, IEEE*

Abstract— Dynamic Spectrum Access (DSA) systems are being developed to improve spectrum utilization. Most of the research on DSA systems assumes that the participants involved are honest, cooperative, and that no malicious adversaries will attack or exploit the network. Some recent research efforts have focused on studying security issues in cognitive radios but there are still significant security challenges in the implementation of DSA systems that have not been addressed.

In this paper we focus on security issues in DSA. We identify various attacks (e.g., DoS attacks, system penetration, repudiation, spoofing, authorization violation, malware infection, data modification, etc.) and suggest various approaches to address them. We show that significant security issues exist that should be addressed by the research community if DSA is to find its way into production systems. We also show that, in many cases, existing approaches to securing IT systems can be applied to DSA and identify other DSA specific security challenges where additional research will be required.

***Index Terms*—Dynamic spectrum assignment, cognitive radio, security, secondary use.**

I. Introduction

DYNAMIC Spectrum Access (DSA) is being proposed as a new communication paradigm to address problems of inefficient spectrum usage [1] [2]. DSA systems that foster secondary use of otherwise idle spectrum can be either decentralized (opportunistic), negotiated (such as market-based secondary use), or based on a regime of license trading. The approach taken by the US Federal Communications Commission (FCC) in [3] epitomizes the opportunistic approach. In this approach, unlicensed users with properly equipped radios can use idle spectrum. The negotiated approach assumes that a license holder explicitly permits a secondary user to temporarily utilize the spectrum (perhaps via a market) [4]. DSA systems that do not rely on secondary use or opportunistic access are those based on spectrum trading where a spectrum license assignments are managed in a market-based environment [5].

An important challenge for all of these DSA methods is security. Most of the research on the operation of DSA systems assumes that the participants are honest, cooperative and that no malicious adversaries will attack or exploit the network. Although some research has been done on security issues related to cognitive radios [6] [7], more challenges related to DSA in all its forms that must be understood before its widespread adoption.

With the FCC's recent *white spaces* decision [3] understanding the security concerns and their mitigation strategies is of increasing importance not just to equipment manufacturers but also to policymakers and end users. Policymakers must ensure that regulations regarding DSA systems are consistent with practical approaches, and that end users are able to make informed choices about how these systems fit into their communication needs.

In this paper, we will first provide an overview of key information security concepts and then discuss the security issues related to DSA systems. In section II we present some information security concept preliminaries. Section III discusses some vulnerabilities in opportunistic DSA and suggests possible approaches that can be used to address them. Section IV describes security issues in negotiated DSA systems and some useful approaches to remediate them. Finally, Section V concludes the paper and discusses possible directions for future research.

II. Security Preliminaries

Information security consists of methods to protect information and information systems resources. The key security goals include *Confidentiality*, *Integrity* and *Availability* (C/I/A).

- *Confidentiality* means ensuring that only authorized people can access a piece of information or resource; sometimes even the existence of the information or resource needs to be hidden from unauthorized entities.
- *Integrity* refers to the trustworthiness and correctness of information and resources – and is commonly referred to as data integrity and origin integrity [8]. *Data integrity* refers to how trustworthy or correct a piece of information is. It is, often simplified as ensuring authorized modification; however, *integrity* of information may be violated also by authorized entities – hence both

Manuscript received December 1, 2009.

Saman T. Zargar, Martin B. H. Weiss, and James B. D. Joshi are with the Telecommunications Program, School of Information Sciences, University of Pittsburgh, Pittsburgh, PA 15260 (emails:{sat47, mbw, jjoshi}@pitt.edu).

Carlos E. Caicedo is with the School of Information Studies, Syracuse University, Syracuse, NY 13244 (email: ccaicedo@syr.edu).

preventive and detective/reactive approaches are needed to ensure data integrity. Origin integrity, often known as authentication, on the other hand, refers to validating that an entity is who it claims to be.

- *Availability* refers to ensuring that authorized entities have timely access to information and resources.

The information security field focuses on ensuring that all these key security goals are met with regard to information that is in storage, being transmitted or being processed. In addition these, issues such as accountability, and non-repudiation are crucial security issues. Accountability refers to ensuring that each activity can be uniquely traced back to the entity which carried it out. Non-repudiation refers to ensuring that an entity cannot deny his actions. Numerous threats and attacks have been identified in information security field that target these protection goals, some of which are listed in Table I.

TABLE I
THREATS AND THEIR C/I/A VIOLATIONS

Threats	C/I/A violations
Eavesdropping: The unauthorized interception of information	Confidentiality
Data modification or alternation: The unauthorized modification of information	Integrity
Denial of Service (DoS): A long-term inhibition of service at source or destination	Availability
Spoofing or Masquerading: Impersonation of one entity by another	Integrity
Repudiation: An entity falsely claims that it did not carry out an activity.	Integrity

III. SECURITY ISSUES IN OPPORTUNISTIC DSA

Cognitive Radios (CRs) are an enabling technology for opportunistic DSA. CRs discover *white spaces* or *holes* in spectrum and opportunistically utilize them without causing interference to primary users [9]. More specifically, Haykin [10] defined CR to be a software-based radio that can sense, learn, adapt and react based on the environment condition. Thus, developing different reasoning and learning algorithms that lead to optimal operation of cognitive radio in a variety of different situations is one of the important goals of the research community.

Operationally, CRs and CR networks must perform the following functions:

- *Spectrum sensing:* detecting spectrum holes.
- *Spectrum mobility:* maintaining seamless communication during the transition to better spectrum.
- *Spectrum management:* selecting the best available channels.
- *Spectrum sharing:* coexisting with other secondary users in one channel.

From the perspective of security, there is little that is unique to cognitive radios from the perspective of confidentiality and integrity[1]. Thus, we focus our attention on availability.

[1] Confidentiality attacks are similar to eavesdropping attacks on any radio system and can therefore be addressed by existing techniques for ensuring confidentiality, such as integrity. The same is true for integrity once a communication has been established between cognitive radios.

It is important to distinguish the context. There are two types of cognitive networks [11]: *centralized* (infrastructure-based) and *distributed* (ad-hoc) cognitive radio networks. In centralized cognitive radio networks, the secondary users are managed by secondary base stations, all of which could be connected through a wire line network. In centralized, infrastructure-based networks, all of the secondary users are synchronized with the base stations, which are also responsible for managing secondary users. Furthermore, the secondary users normally cooperate in spectrum sensing and sharing tasks; although non-cooperative centralized cognitive radio networks may also exist.

In distributed cognitive radio networks, secondary users use ad-hoc communication and mesh networking concepts. Each set of secondary users who are in range of each other can exchange information directly. The secondary users who are not within the communication range of each other can exchange information by relaying through other nodes in the network. Secondary users in distributed cognitive radio networks are responsible for determining their transmit power, spectrum band, etc., in accordance with spectrum regulations.

In distributed cognitive radio networks, cooperation between all the secondary users may occur via mechanisms such as control channels, etiquette rules or explicit message exchange. Secondary users in these networks may also use a non-cooperative approach, in which each secondary user optimizes locally and may compete with others in doing so.

Security issues could be a serious roadblock to a successful adoption of this new technology in production systems. In this section, we present various security issues in opportunistic DSA systems. We will address attacks on each of the major functional areas described above.

A. Attacks on Spectrum Sensing and Sharing

Attacks on spectrum sensing and sharing are most often DoS attacks (see Table I). In [7], Jakimoski et al. show that the majority of CR-based DSA implementations are unable to offer both minimal disruption of the primary users and efficient utilization of the vacant spectrum bands when a malicious adversary is introduced. They analyze two different topologies: a *centralized secondary network* (infrastructure-based cognitive network) and a *distributed secondary network* (ad-hoc based cognitive network) using a channel evacuation protocol. In the centralized secondary network, they augment a spectrum pooling system with a boosting protocol to detect idle spectrum and inform other secondary users about it [7] [12] [13]. Attackers can spoof the secondary users to use spectrum bands that are not idle, and therefore disrupt the services of the primary network, or make other secondary users evacuate the spectrum and inhibit their usage of the idle bands.

Furthermore, in both centralized and distributed opportunistic DSA systems, it is possible to have more than one secondary network. Hence, the effects of the attack become even worse and transmission from malicious users in one network can also cause disruption of service to the primary and secondary users of the other networks, this type of attack is referred to as an overlapping secondary user attack [11]. Researchers have proposed several strategies to mitigate these attacks:

- *Modifying the modulation scheme*: Using spread spectrum techniques such as frequency hopping [14] and direct-sequence spread spectrum [15], make it more difficult for attackers to launch effective DoS attacks, although they may be able to degrade service quality.
- *Detection and prevention* of attacks using passively obtained data, such as observing the primary user's location and signal characteristics [9].
- *Using authentication and trust models*. In [16], Wang et al. propose a malicious user detection algorithm that calculates the suspicion level of secondary users based on their past reports and then based on that calculates trust and consistency values to eliminate the malicious users' influence on the primary user detection results. They effectively differentiate between malicious and honest secondary users based on the proposed trust value indicator.

B. Attacks on Spectrum Mobility (The handoff process)

The main objective of spectrum mobility function is to ensure seamless communications when a CR vacates a channel and moves to a new channel. Normally, a CR will vacate the current band if it is no longer available, when the quality degrades, or when the user moves from one place to another. In order to maintain the communication path, the CR needs to select a new appropriate spectrum band, and move to it immediately. The spectrum handoff process begins with a CR vacating the current spectrum band and ends when the CR moves to the new band [1].

A failed handoff may require a long recovery time and can cause upper layer protocols to fail, which affects availability. There are several possibilities in which the handoff process might be disrupted. In one kind of disruption, an attacker can compel a CR to vacate the current band by masquerading as the primary user (Primary user emulation) [17]. In a primary user emulation attack, an attacker sends primary-user-like signals during the spectrum sensing period and thus jams the secondary user. To mitigate this kind of attack, a secondary user can randomly hop over multiple channels. This opens a tradeoff between choosing good channels and evading an attacker's jamming when different channels have different qualities (e.g. probabilities of being idle, propagation characteristics, etc.). The interaction between the secondary user and the attacker has been called a *dogfight in spectrum* due to the dynamics of pursuit and evasion [18]. In [18], Li et al. analyzed one-stage and multi-stage cases by numerical simulation results and they showed that the performance of a secondary user was improved when the number of channels was increased or the channel state certainty was reduced.

Another type of disruption occurs when the attacker jams the network to increase the time needed to select a new available band or cause a communication failure [19]. Mitigation requires broadening the operating range of the CR, which increases costs and energy consumption.

Finally, if an attacker can take control of the common control channel that some CRs use [20], s/he can change the key parameters of the available band or interfere with primary users. Hence, this kind of attack prevents spectrum mobility. Mitigating this attack requires securing the control channel using standard authentication, authorization, and auditing (AAA) techniques.

C. Attacks on Spectrum Management

CRs detect idle spectrum bands for communication using spectrum sensing. Their spectrum management function will then select the most appropriate bands considering the QoS demands of the users. In [1], the functions of spectrum management are classified as spectrum analysis and spectrum decision. Spectrum analysis provides the characterization of different spectrum bands and the spectrum decision process selects the appropriate spectrum band for the current transmission by considering the QoS requirements and the spectrum characteristics.

Spectrum sensing data falsification attacks are a serious threat to the spectrum analysis process and can impact the results of spectrum decision function, which can lead to reduced system performance. In this kind of attack, a malicious user sends false local spectrum sensing results to a data collector in a cooperative sensing system. The results are then propagated to other CRs in the system, which may lead to a suboptimal spectrum use decision resulting in degraded system performance.

The attacks in these kinds of systems are even worse than for independent CRs because it will affect other base stations or users in the network, causing the whole system to misbehave [21]. For example, in an IEEE 802.22 CR network, if the adversary mimics a television signal, then the station detecting this signal will propagate this observation to every station in the network causing all secondary users to evacuate the spectrum. In [22], Frangoudis et al. analyzed incentives for truthful distributed (cooperative) spectrum sensing and reporting relevant attacks. As a solution for spectrum sensing data falsification attacks, they offer an efficient filtering scheme by using information (spatial and temporal) from multiple sources to filter out false reports by applying simple majority or voting rules. As a result, collected reports can easily detect "odd" spectrum measurements. However, they do not consider the effect of hidden nodes on this strategy. If majority of the voting stations are hidden nodes, a false negative could still result.

This research suggests that a variant on this kind of attack might be an opportunistic CR in a cooperative system that self-optimizes. That is, a radio in a cooperative sensing system may decide to send out false information that would cause other radios in the network to change their spectrum use behavior, allowing the selfish radio to improve its own communications channel. Such an attack could avoid AAA techniques that might filter out intruders. A voting system as described above may be effective in isolating selfish nodes, especially if a punishment strategy is adopted by the network.

D. Attacks against the Learning Engine

CRs are built to respond to their environment, so some may employ artificial intelligence (AI) techniques in their decision making. Thus, it is important to consider attacks that focus on exploiting these techniques, which may use learning engines to react to their environment based on past and present information. For example, a reasonable strategy for attacks on spectrum sensing would be to distort the information used by

the algorithms that separate false from correct sensing results. Such algorithms would almost certainly need to consider historical sensing results. If a patient attacker were to persistently feed the intelligent CR with false results, the false results would become part of the "known" historical facts, which would be persistent over time. The patient attacker would then achieve a rather long lasting DoS attack. Such an attack worsens when we have a cooperative network since the fallacious information (and belief network) will propagate through the network and thus becomes even more persistent over time.

Mitigation of these kinds of attacks is rather challenging. One approach is to make the task of the patient attacker more difficult by being more critical of the accepted information and another is to decrease the persistence of beliefs (that is, to allow only short term results) [7]. Yet another approach is to define trust metrics [21] and letting radios reason about the trustworthiness of their neighbors. All of these mitigation strategies limit the effectiveness of the AI in the CR.

Another kind of attack on the learning engine requires an attacker to tamper with the system and modify its policies. For instance, a system may have a policy to evacuate the spectrum whenever it detects the primary user's existence. If an attacker can gain access to the policy engine, s/he can program the radio to "exploit" instead of "evacuate" the channel. Hence, we need tamper proof radios to address this issue.

E. Attacks on Spectrum Sharing

The vulnerabilities described above require physical layer attacks. Opportunistic CRs require a MAC layer to enforce the sharing of spectrum holes among several users. He and Mitchell [23] catalog the security vulnerabilities of 802.11i. It is reasonable to assume that many of the vulnerabilities and mitigation strategies suggested by the authors would have to be addressed in the MAC for opportunistic CRs as well. Since these security challenges are not specific to CRs but rather to MAC layers in general, we will not address them in this paper.

Most of the secondary users in CR networks are mobile and have limited resources and processing power. Hence, providing secure cognitive radio capability in real-time is a challenging task. In doing so, light weight security protocols are required especially for power/resource constraint environments [11].

Furthermore, as the number of opportunistic users in opportunistic DSA increases, the networks become more vulnerable to the aforementioned attacks. Thus, it becomes increasingly important that secure approaches be applied. This kind of MAC-based opportunism was examined by Sandvig [24], who showed that system availability existed even in such a rivalrous environment.

IV. Security in Negotiated (Cooperative) DSA

Opportunistic DSA systems are characterized by the absence of coordination between the primary and secondary user. If a primary user (i.e., a license holder) must make investments to ensure the security of their system to mitigate risks of opportunistic use of their spectrum, then we may expect them to make their channels appear busy (by sending null characters, for example) if the cost of transmitting these characters is less than the required security investment.

If we assume that secondary spectrum sharing is the result of an explicit agreement between the primary and the secondary user, then the operational environment changes, as do the security concerns. In negotiated DSA, we could expect to see more spectrums available for sharing. Furthermore, because many of the sophisticated functions of cognitive radios are not required, we could imagine that negotiated systems can use cheaper, more energy efficient and (possibly) more secure software radios.

In considering the security aspects of negotiated DSA, it is also important to be mindful that a primary user may have commitments to its (regular) users. These commitments may include a Service Level Agreement (SLA) that defines monetary penalties for non-performance.

The threats outlined in Table I apply in negotiated DSA albeit with some differences because these systems are rooted in commerce. Eavesdropping and data modification attacks are no different in negotiated and opportunistic DSA so we will not discuss them further. In negotiated DSA, it is useful to distinguish monetary or financial threats from technical ones.

Because of the potentially commercial nature of negotiated DSA, some of the threats involve the terms and conditions of contracts. These can include price and performance requirements (such as an SLA). A primary user may choose to incur the penalty if a sufficiently attractive alternative arises. A secondary user may choose to renegotiate (or even repudiate) an agreement if the demand motivating the spectrum request unexpectedly evaporates. In the former case, the secondary user will be denied service whilst in the latter case the primary user will be denied revenue. Thus, it can be classified as a commercial threat. In cases involving renegotiation, no technical remedies exist.

However, repudiation, DoS and spoofing deserve some attention:

- *Repudiation* – Repudiation may take on an additional meaning in negotiated DSA. A primary or secondary user may choose to deny the existence of a negotiated contract.
- *Denial of service* – A malicious third party may use a variety of techniques to prevent primary or secondary users from achieving their communications or systems goals. In negotiated DSA, DoS attacks can have economic consequences because of penalties that might be associated with service level agreements (SLAs). While this may be dealt with in contracts, it may also be necessary to implement technical mechanisms to distinguish externally and internally sourced events.
- *Spoofing* or *man-in-the-middle* attacks can be used by malicious third parties for eavesdropping, data modification, or creating the appearance of repudiation.

Regardless of the mechanisms used to achieve the agreement (i.e., brokers, markets, etc.) the following functions must occur for negotiated DSA:

- *Primary and secondary users must find each other (Advertisement).* Primary users may announce the availability of spectrum through an advertisement of some kind, and secondary users must respond to one or more advertisements.

- *An agreement must be negotiated*. The terms of this agreement may include spectrum boundaries, geographical boundaries, start and end times, price, penalties for failure to perform, etc.
- *Sharing and monitoring*. The sharing occurs under the terms of the contract. One or both parties may choose to monitor the performance of the other party to ensure compliance.
- *Settlement at the end of the sharing episode*. When sharing is complete, settlement procedures may be necessary to complete the terms of the contract. Settlement may include payment of service fees and penalties, updating trust models, publicizing the terms of sharing, etc.

We organize the remainder of this section around the four functions outlined above plus some additional comments.

A. Advertisement

Before a contract can be established, the primary and secondary users must first find each other. This can be achieved in a number of ways, including:

- Registering in a (hypothetical) secondary use market as a primary or secondary user
- Registering with a broker
- Opening or responding to a directory listing

Since secondary use is a contractual outcome, primary and secondary users must be able to authenticate the legitimacy of their counterpart to avert subsequent spoofing or man-in-the-middle attacks. While repudiation is not a concern at this stage because no contract has yet been made, DoS attacks are possible if registries are overwhelmed with requests.

B. Negotiation

Once a secondary user has identified a potential primary user, a negotiation must occur on the parameters of the secondary use. This can involve specifying the amount of bandwidth required in a particular frequency band, the geographical boundaries over which this secondary use can take place, the start and end time of the secondary use, the fees paid by the secondary user to the primary user, SLAs that may specify the amount of noise power permitted in the time-space-frequency dimension outlined above, penalties for violating the SLA, etc.

A threat to this operational phase is causing the negotiation overhead to increase. Such an increase can come as a function of time or resources expended. As such, it can be a form of DoS attack. The form of this threat varies based on the mechanics of the negotiations.

In bilateral negotiations, increased negotiation overhead can occur if many special considerations are added or if negotiations are opened with no intent to conclude an agreement. This is a form of DoS because it consumes resources of primary users and may lock up spectrum resources during the negotiations that might be used by other spectrum users.

Mitigation strategies for this kind of attack include building trust models and authentication. In trust based approach, negotiations may be rejected if the trust levels are not sufficiently high. Trust levels are incremented upon successful negotiations and decremented upon unsuccessful ones. Thus, they are historical and not current representations of behavior. Thus, a patient malicious user could build a high trust level that could be leveraged in future for a DoS attack of this kind. There exist several trust negotiation approaches in the literature (e.g., those reviewed in [25]) that address trust negotiation in a slightly different context. Such techniques have explored trust computation based on reputation, recommendation and other factors such as risk, and cost [25]. These may be adopted to build a trust based negotiation approach for cooperative DSA.

C. Sharing and Monitoring

After an agreement has been concluded, spectrum sharing begins at the time specified in the agreement. Primary users do not transmit on the spectrum during the specified time period and the geographic area while secondary users do. During this phase, both primary and secondary users may choose to monitor the behavior of the other party to the agreement to ensure that SLA terms (if any) are satisfied.

During this phase, a malicious third party, who may have discovered the details of the agreement through eavesdropping, may, masquerading as the primary user, transmit in the secondary users' spectrum. If the channel is monitored, it would appear to be a repudiation of the contract by the primary user to the secondary user and would also be a DoS for the secondary user. Arbitration may be necessary to resolve this during the settlement phase, or a "fingerprinting" approach to distinguish primary users from third parties masquerading as the primary user.

A malicious third party could also engage in DoS by jamming the spectrum during the contract period. Unlike opportunistic secondary use, where the secondary user can relatively easily utilize frequency hopping to avoid the jammed band, the secondary user is helpless if the negotiated contract specifies the use of a specific channel. Mitigating this kind of attack would require a contract that makes a set of channels available over which the secondary user can frequency hop. This raises the cost of negotiating over a simple secondary sharing contract since the contract is more complex

D. Settlement

After the secondary use period is concluded, the contract is closed and the primary and secondary users settle. This may include monetary payments for spectrum usage rights and/or penalties for failing to satisfy the terms of the SLA. The settlement phase is vulnerable to third parties who would seek to capture the revenue flows and/or influencing the trust levels of the primary and secondary users.

Capturing the revenue flows is an important concern in negotiated secondary use DSA. The attacks and mitigation are similar to those that have been developed for electronic commerce [26] there is little that is specific to DSA.

If the system uses a trust-based approach, a malicious attacker may seek to influence the trust levels of the primary and secondary users. The motivation for this is manifold and may involve influencing the prices for secondary use or the amount of available spectrum in the future. Applying AAA techniques to the trust reporting can mitigate some of these risks.

E. Additional comments

While not a security issue with negotiated DSA, service theft is a security issue of some importance to commercial operators. A good example of poor security practices leading to service theft can be seen in early cellular systems. In these systems, electronic serial numbers (ESNs) and Mobile Identification Numbers (MINs) were transmitted as plain text and were subsequently captured and programmed into rogue phones [27]. Subsequent mobile systems have implemented stronger communication security technologies.

V. Security in Spectrum Trading based DSA

In a spectrum trading market, the market participants must register with the spectrum exchange or a broker to participate in the market. Thus, by not having opportunistic secondary use and using a user/identity registration mechanism, many security problems are avoided. However, vulnerabilities in the trading protocol may result in incorrect information submission at the time a trade is being made and could seriously impact market behavior. For example, consider a replay attack, where a malicious node replicates the messages to announce a market participant's willingness to sell or buy spectrum. If it is not detected, the behavior of the market and the liabilities of the market participant would be affected. Also, the presences of malicious nodes that generate interference within the set of tradable frequencies in a given region are a key security issue. The generated interference would diminish the value of spectrum but malicious nodes could be detectable by collaborative methods among the entities trading spectrum in a region thus reducing the effect of the attack. In the extreme, it could affect the availability of the communications channel In general, as with negotiated secondary use; spectrum trading DSA markets are susceptible to spoofing and DoS attacks.

VI. Summary and Future Work

In this paper, we have presented an overview of the security issues in DSA environments. Most of the recently proposed implementations for DSA networks assume that the participants involved in the protocols are cooperative and that there are no malicious adversaries that want to attack the network. Hence, most of the proposed solutions are vulnerable to several attacks on the primary and secondary user's networks.

With the FCC's recent, "White Spaces" decision, understanding the security concerns and approaches to address them is of increasing importance not just to equipment manufacturers but also to policymakers and end users. Policymakers must ensure that regulations regarding DSA systems are consistent with practical approaches, and that end users must be able to make informed choices about how these systems fit into their mix of communication technologies.

Convincing spectrum owners to implement security in a negotiated DSA environment should be possible since the service providers are being compensated for the service provided. Adoption of secure negotiated DSA techniques would generate competition among providers as they can offer attractive, secure products via competitive pricing. This option is a more "business friendly" approach than the simple opportunistic DSA in which, though the services are free, they are not regulated or guaranteed to be secure.

A key future work is to design protocols for secure implementations of negotiated DSA and opportunistic DSA network functions. Future research must be focused on vulnerabilities and remediation of specific systems and protocols.

References

[1] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks : A survey," *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 50, no. 13, pp. 2127-2159, September 2006.

[2] M. M. Buddhikot, "Understanding Dynamic Spectrum Access: Models, Taxonomy and Challeges," in *IEEE DySPAN*, Dublin, Ireland, April 2007.

[3] FCC ET Docket No. 08-260, "Second Report and Order and Memorandum Opinion and Order -- Unlicensed Operation in the TV Broadcast Bands / Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3GHz Band," *US Federal Communications Commission, Washington DC, FCC 08-260*, 2008.

[4] A. Tonmukayakul and M. B. H. Weiss, "A study of secondary spectrum use using agent-based computational economics," *Springer's NETNOMICS journal*, vol. 9, no. 2, pp. 125-151, Oct 2008.

[5] C. Caicedo and M. B. H. Weiss, "On the Viability of Spectrum Trading Markets," in *Telecommunications Policy Research Conference (TPRC)*, Arlington, VA, September 2009.

[6] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in *CROWNCOM'2008*, Singapore, 2008, pp. 1-7.

[7] G. Jakimoski and K. P. Subbalakshmi, "Denial-of-Service Attacks on Dynamic Spectrum Access Networks," in *ICC Workshops'08*, Beijing, May 2008, pp. 524-528.

[8] M. Bishop, *Introduction to Computer Security*, first Edition ed.: Addison-Wesley Professional, November 5, 2004, ISBN-10: 0321247442.

[9] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *IEEE Workshop on Networking Technology for Software Defined Radio Networks (SDR)*, Reston, VA, Sep. 2006, p. 110– 119.

[10] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE Journal on Selected Areas in Communication (JSAC)*, vol. 23, no. 2, pp. 201- 220, February 2005.

[11] Qusay H Mahmoud, Ed., *Cognitive Networks - Towards Self-Aware Networks*.: John Wiley & Sons, 2007.

[12] T.A. Weiss, J. Hillenbrand, A. Krohn, and F.K. Jondral, "Efficient signaling of spectral resources in spectrum pooling systems," in *10th Symposium on Communications and Vehicular Technology (SCVT)*, Eindhoven, 2003.

[13] T.A. Weiss and F.K. Jondral, "Spectrum pooling: an innovative strategy for the enhancement of spectrum efficiency," *IEEE Radio Communication Magazine*, vol. 42, no. 3, pp. S8-14, Mar 2004.

[14] P. Popovski, H. Yomo, and R. Prasad, "Strategies for Adaptive Frequency Hopping in the Unlicensed Bands," *IEEE Wireless Communication*, vol. 13, no. 6, pp. 60-67, December 2006.

[15] NTIA, "Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook)," January 2008 Edition.

[16] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaboration spectrum sensing in cognitive radio networks," in *CISS*, Baltimore, MD, March 2009.

[17] R. Chen, J. M. Park, and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 26, no. 1, pp. 25 - 37, January 2008.

[18] H. Li and Z. Han, "Dogfight in Spectrum: Jamming and Anti-Jamming in

Multichannel Cognitive Radio Systems," in *IEEE Globecom 2009*, Honolulu, Hawaii, November 2009.

[19] Yuan Zhang, Gaochao Xu, and Xiaozhong Geng, "Security Threats in Cognitive Radio Networks," in *10th IEEE International Conference on High Performance Computing and Communications (HPCC'08)*, Dalian, 2008, pp. 1036-1041.

[20] Simon Delaere and Pietre Ballon, "Multi-level Standardardization and Business Models for Cognitive Radio: The Case of Cognitive Pilot Channel," in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Chicago IL, 2008, pp. 1-18.

[21] T. C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," in *CrownCom'08*, Singapore, May 2008.

[22] P. A. Frangoudis, S. Arkoulis, G. F. Marias, and G. C. Polyzos, "Incentives and Security Considerations in Distributed Spectrum Sensing," in *1st Euro-NF Socioeconomics Workshop, , Greece, October 2008*, Athens, October 2008 (extended abstract).

[23] Changhua He and John C. Mitchell, "Security analysis and improvements for IEEE 802.11i," in *Proceedings of the 12th Annual Netwkr and Distributed System Security Symposium*, 2005, pp. 90-110.

[24] Christian Sandvig, "The Return of the Broadcast War," in *Telecommunications Policy Research Conference*, Arlington VA, 2005.

[25] Y. Zhang and J. B. D. Joshi, "Access Control and Trust Management for Emerging Multidomain Environments," in *Information Assurance, Security and Privacy Services*, H. Raghav Rao and Shambhu Upadhyaya, Eds. UK: Emerald Group Publishing Limited, 2009, ch. 15, pp. 421-455.

[26] W. Ford and M. S. Baum, *"Secure electronic commerce: building the infrastructure for digital signatures and encryption"*.: Prentice Hall PTR Upper Saddle River, NJ, USA, 2000.

[27] Michael J Riezman, "Cellular Security: Better, but foes still lurk," *IEEE Spectrum*, vol. 37, no. 6, pp. 39-42, June 2000.