Recent Security Issues on Cognitive Radio Networks: A Survey

Sterling Holcomb
Department of Electrical Engineering
Georgia Southern University
Statesboro, GA 30460, USA
Email: nh01141@georgiasouthern.edu

Danda B. Rawat
Department of Electrical Engineering
Georgia Southern University
Statesboro, GA 30460, USA
Email: db.rawat@ieee.org

***Abstract*—Cognitive radio networks are a method for improving wireless communications with radios that can adapt their operating parameters to cope with changes in their environment. This flexibility enables radios to perform with greater throughput, robustness, and field updatability than traditional wireless communication devices; unfortunately, it also presents several security challenges unique to cognitive radio networks and new angles for traditional attacks. These threats can be classified into radio configurability and cognitive radio behavioral vulnerabilities. In this paper we explore specific threats to cognitive radio networks and their countermeasures from literature. With this paper, readers can have a thorough understanding of cognitive radio network security and the research trends in this area.**

I. Introduction

Cognitive radio networks are an emerging technology to optimize the use of the electromagnetic spectrum for wireless communications. Before we proceed, certain essential definitions must be understood. A cognitive radio (CR) is a radio that can learn about its environment from statistical analysis of the radio spectrum and adapt its operating parameters to achieve highly reliable, spectrally efficient communication [1], [2]. Similarly, a cognitive radio network (CRN) is formed by multiple CR nodes communicating with each other. In order to intelligently adapt to their operating environment, CRs must be able to configure themselves in real time; therefore, unlike traditional radios, these devices cannot define their physical layer operations with circuitry. Software defined radios (SDR) are devices "in which some or all of the physical layer functions are software defined" including: field programmable gate arrays, digital signal processors, general purpose processors, and programmable system on chips [3]. Thus SDR is a key building block to CR. Finally, Dynamic Spectrum Access (DSA) is the method of using CR to implement secondary users on licensed bands without adversely effecting licensed primary users. This method fills in the time variable, unused portions of licensed frequency bands with secondary transmissions [4], [5].

Cognitive radio networks are an answer to the growing overcrowding of unlicensed communications bands. Since the advent of license-exempt bands from the FCC–particularly with the implementation of IEEE 802.11 [6] protocols into innumerable mobile devices–the use of wireless communications in unlicensed bands has increased tremendously. Despite the growing overcrowding of these unlicensed frequencies, there are several licensed bands which remain idle most of the time. CRNs are a way to safely allow secondary users to access those frequencies without interfering with primary users [7]–[9].

Like any modern communication system, CRNs must be secure to be useful. In other words, CRNs must guarantee the confidentiality, integrity, and authenticity of data traveling through the network [3] [7] [10], [11]. Unfortunately, in addition to the many types of security challenges faced by traditional radio networks, CRNs must account for attacks designed to exploit their adaptive nature.

This paper is a survey of the unique threats facing CRNs, traditional attacks modified for CRNs, and countermeasures for these threats. It is organized as follows. Section II details the security requirements of CRNS. Section III covers the vulnerabilities introduced by the configurability of cognitive radios. Section IV relates countermeasures for the threats in III. Section V contains the vulnerabilities to CRNs due to CR Behavior. Section VI offers countermeasures to the threats in V. Section VII covers the open research areas in CRN security. Finally, Section VIII concludes the paper.

II. Security Requirements

Many organizations have defined security requirements for communications networks. For the purpose of this paper we will selectively consider guidelines published by the National Security Agency (NSA). The NSA's definition of information assurance is the set of "measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" where availability is the ability to access the data at a given time, integrity is guaranteeing the data is unaltered, authentication is the process used to verify the entity accessing the data, confidentiality is the promise that only authenticated users with permission can access the information, and non-repudiation is the commitment to preventing any entity that alters data from denying their identity or actions [3], [11], [12].

Looking beyond the security requirements of the data transported and stored in a network, the resources of a CRN must also be preserved. Accordingly, we extend the NSA's security

978-1-5090-2246-5/16/$31.00 ©2016 IEEE

recommendations to arrive at this paper's requirements for CRN security [3].

1) The system will verify the identity of any entity using the network.
2) The system will verify the permissions of an entity to access resources and perform actions.
3) The integrity of the system and its components will be guaranteed.
4) The integrity of the data in the system will likewise be guaranteed.
5) Stored and transmitted information will remain confidential.
6) The system will prevent entities from denying their actions.
7) The system will comply with the appropriate regulations.

CRNs that comply with these requirements should be able to address the security threats that have been discovered to attack CRNs [3] [10].

III. Radio Configurability Vulnerabilities

Cognitive radio networks rely on SDR to configure themselves for their operating environment dynamically and intelligently. This is advantageous because the network's capabilities can be extended in the future by software updates containing new operating modes or applications [7]. Unfortunately this feature is accompanied by the classic Achilles heels of software updates: the uncertain credibility of the source and quality of the new software [3]. The following sections detail specific threats that take advantage of the configurability of CRNs.

A. Eavesdropping Attacks

Eavesdropping attacks are incumbent to wireless communications since their only prerequisite is access to the medium [13]. These attacks involve a malicious node listening to transmissions between legitimate members of the CRN [14]. In traditional networks these threats seek user data as it is being transmitted over the network. Eavesdroppers on CRNs have the further goals of obtaining configuration [15] and waveform data [3].

1) Configuration Extraction: This type of eavesdropping attack involves malicious devices attempting to determine how a CRN node is setup [3] including: control channel parameters [16], spectrum analysis methods, channel-state information estimation protocols, and transmit-power control techniques [1]. While eavesdropping on transmissions does not directly damage the operations of a CRN network, it enables future attacks to be more effective by targeting the operation of this specific network.

2) Waveform Data Extraction: Much like configuration extraction threats, waveform data extractions are eavesdropping attacks. Waveforms, the target data, are the software implementation of a communications service like GSM or IEEE 802.11 [3]. This data can be used for various malicious purposes including future man in the middle attacks or node identity spoofing attacks.

3) User Data Extraction: These threats represent the end goal of many attackers. In user data extraction attacks, eavesdroppers record all network traffic in the hope of gathering information to aid in identity theft or subsequent attacks [3]. Among the data targeted in these attacks are: usernames, passwords, credit card numbers, banking information, web history, and personally identifying information.

B. Maliciously Corrupted Upgrades

This type of attack focuses on inserting malicious executables or supporting files on CRN nodes [3]. In traditional wireless communication devices the impact of corrupted upgrades is limited since the physical layer parameters of a device are defined in hardware; however, most of these parameters are defined in software for cognitive radios. Thus the configurability of CRN nodes opens up new targets for attack [10].

1) Malicious Software Injection: Essentially, this threat is inserting malicious code to run on a node. The infection vectors of these threats do not differ significantly for CRN nodes and traditional platforms like mobile phones, but, the importance and frequency of updates is greater for CRNs. CRNs depend on software updates to expand their functionality and improve their ability to adapt to their environments; since these are primarily software defined platforms, upgrades can be implemented cheaply in the field [3].

2) Unauthorized Waveform Masking: The distribution of authorized waveforms is an essential task in initializing and maintaining a CRN since they define the interaction protocols for clients and base stations. Accordingly these attacks represent one of the most dangerous threats to CRNs, the distribution of a malicious waveform under the guise of an authorized waveform. If successful, these attacks can disrupt CRN operations and even interfere with traditional wireless networks [3].

C. Malevolent Software on Nodes

These threats identify the targets of malicious software residing on CRN nodes [3]. As personal computers have proven, it is nearly impossible to detect and prevent all of the bugs and Trojan horses in complex software. Since CRN nodes are implemented using SDR they are also vulnerable to malicious software. The end result of these breaches is a loss of functionality and possibly illicit RF transmissions [17].

1) Configuration Data Corruption: This threat is to the integrity of the information provided to the node to configure its functionality [3] including: control channel parameters [16], spectrum analysis methods, channel-state information estimation protocols, and transmit-power control techniques [1]. A node could be rendered inoperable by ineptly altering or deleting this configuration information. More skilled alteration of this configuration data could cause the node to transmit in violation of local regulations or in such a way that it compromises the other users of the network.

2) Unproductive Resource Consumption: Since CRNs rely on SDR, each node on the network must have computational resources. This threat expends those resources unproductively in order to impair a node's functionality and disrupt traffic in the network [3] [7].

3) Waveform Code Corruption: In SDR, waveform codes are the software implementations of interaction protocols for base stations and clients such as GSM. This threat is to the integrity of one or more waveforms stored in the node [3]. The impact of this type of attack can range from loss of functionality in the case of waveform deletion to data and network throughput loss when waveforms are modified to allow unauthorized users access to the network.

4) Unauthorized Use of SDR Services: This attack deals with entities attempting to obtain access to services for which they are not authorized. Examples of potentially impacted services include: cryptography, waveform operations, and CRN resource distribution. The consequences of these misappropriations depends on the service that has been co-opted and includes the violation of all of the security requirements identified in Section II [3] [18].

IV. Radio Configurability Countermeasures

Section III introduced the attacks on cognitive radio networks that are unique to CRNs or modified to target CRNs due to the unusual amount of configurability CRN nodes must posses to operate. This section presents countermeasures to those attacks from both solutions for traditional wireless networks and research specifically into CRN security.

A. Eavesdropping Attacks

Within the category of eavesdropping attacks there are two distinct goals: directly obtaining user data [13], and discovering how the cognitive radio works [3]. The first of these goals, targeting user data, is a threat that is not unique to CRNs. User data eavesdroppers can be foiled by encrypting the data stream between two authenticated users. This architecture is described in [19] but the recommended encryption algorithms have since been proven to be susceptible to brute force attacks with modern hardware [13]. More secure encryption algorithms such as triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) are described in [20]. Furthermore, there is an inherent secrecy rate to cognitive radio transmissions due to differences in interference and noise at the eavesdroppers' locations and the legitimate users' locations. Different schemes have been proposed in [14], [21], [22], [23], [24], [25], and [26] to maximize this secrecy rate.

Beyond gathering user data, eavesdroppers on CRNs seek to learn how the nodes are configured as well as what waveforms they are implementing [3]. Since this channel state information is observable by all with access to the medium [13], encryption is not an effective countermeasure. Instead, secrecy rate maximization techniques identified in the previous paragraph should be implemented to mitigate these threats [22].

B. Maliciously Corrupted Upgrades

Since only the frequency and importance of updates for CRNs–rather than the attack vectors of these threats–differ from those traditional networks encounter, this problem of securely downloading software has commercially established solutions that must only be adapted to CRNs. The most common technique for verifying the integrity and authenticity of a software update is a digital signatures consisting of a hash and encryption function added to the software download to verify the authenticity of the patch. Before transmission over the network, the entire software package and signature is symmetrically encrypted using a secret key stored in each CRN node. Since only the destination node has the key, the integrity of the update is insured [3] [7].

An alternative method to signing and encrypting the update is to transfer the update over a secure connection between a trusted source server to the device using a protocol like Light Secure Socket Layer (LSSL). LSSL is a version of traditional SSL modified to reduce the bandwidth of the communication and transfer the majority of cryptographic related computations to the server [3] [7] [27]. This allows secure links to be formed with client devices containing limited computational and networking resources, such as a CRN node who's resources are dominated by CR activities like spectrum sensing [21].

C. Malevolent Software on Nodes

In order to guard against and limit the scope of malicious or malfunctioning software CRN nodes must implement a security architecture. Several such architectures have been proposed in literature. One architecture, introduced in [17], consists of an automatic calibration & certification unit (ACU), GPS receiver, and radio security module (RSM). The ACU is a non-reconfigurable hardware module that resides between the software layers and the CR output. It analyses the node's output and restricts that signal based on the regulations for its present location as identified by the GPS. This limits the potential harm from co-opted nodes. The RSM portion of the module is also referred to as a security administrative module in [3] and secure radio middleware in [18]. Like the ACU, it is implemented on non-reconfigurable hardware to prevent tampering [17] or software to preserve reconfigurability [18]. This portion of the architecture manages the entire life cycle of software on the node from downloading through instillation and operation to termination.

Another CRN security architecture, called trusted computing (TC), is established in [28]. This approach is based on determining the trustworthiness of systems and subsystems in a manner similar to how humans decide to trust each other. These processes are identified as "either first hand experience of consistent behavior, or trust in someone who vouches for consistent behavior; unambiguous identification; and unhindered operation" [28]. This goal is accomplished by integrating an implementation of a system similar to the RSM of [17] into the operating system of a CRN node.

V. Cognitive Radio Behavior Vulnerabilities

Traditional wireless communication systems are limited by their hardware and firmware to operate according to strict standards and spectrum allocations. Unlike these systems, CRNs have the ability to communicate in a wide range of frequencies and are capable of altering their parameters at runtime to cope with sensed changes in the environment [1]. If a CRN node were to be taken over by an attacker, then these features could be misused to cause great harm and disruption to the communication infrastructure. Furthermore, most research assumes that nodes act logically and selflessly to arrive at an optimal spectrum utilization. If malicious nodes are on the network, then this activity can be disrupted by injecting false spectrum sensor data to gain a performance advantage for themselves [3]. More directly, if a CRN node has been compromised, then it can be used to carry out jamming attacks targeting service or control channels of spatially close primary user networks or the CRN itself [3] [7] [10] [29] [30]. The following sections detail specific threats that exploit the vulnerabilities introduced by cognitive radio behaviors.

A. Denial of Service Attacks

Jamming attacks, like eavesdropping attacks, are a perennial problem in wireless communication systems [7]. These threats seek to disrupt network performance by flooding the spectrum used by the network with high power interference. Though denial of service (DoS) attacks on CRNs do not yet significantly differ from those faced by traditional networks, cognitive behaviors can be designed to greatly improve network performance in the presence of jammers [10].

1) Jamming the Cognitive Control Channel: When CRN nodes cooperate and share spectrum information the network converges on the optimal spectrum utilization condition more quickly. This threat seeks to block CRNs' ability to share control information by jamming the network's control channel [3] [7] [10] [29]. This attack requires the aggressor to know the frequency of the control channel, but this can be determined by an eavesdropper analyzing traffic sent from one or more nodes.

2) Jamming the Most Active Band: During operation of a CRN it is common for particular radio frequency bands to experience flashes of activity. In a most active band (MAB) attack a malicious agent attempts to detect these hot spots and jam them in order to impair network function [30]. This is essentially the inverse of the operation performed in DSA by a properly functioning CRN node when looking for an unoccupied frequency on which to transmit [4] [30].

B. Greedy Attacks

A common assumption in non-security related CRN research is that CRN nodes will make logical altruistic decisions [3]. Greedy attacks violate this assumption by seeking an unfair amount of resources for themselves at the expense of collective performance [31]. This section relays the common attack vectors for these threats.

1) Malignantly Changing Cognitive Control Messages: If a malicious node were greedy, then it could alter cognitive control messages before forwarding them in order to manipulate bandwidth allocations. Alternatively, malignant nodes could deny requests to specific nodes or groups of nodes in order to impair the network's functionality. Given the opportunity, such a node could even manipulate other networked stations to transmit or receive in such a way that they are more vulnerable to deeper attacks by the malicious node or its cohorts [3] [15].

2) Stealing a Primary User's Identity: Due to the flexible nature of CRN nodes, they are capable of imitating primary users if taken over for malicious purposes [7] [10] [32]. This kind of threat consists of an actor transmitting in a pattern that other CRN nodes will recognize as a primary user [10]. These attacks can be either a selfish attempt to gain a quasi reserved band for communication [29] or a sophisticated jamming technique to deny the use of the band to secondary and real primary users [3].

3) Stealing a CRN Node's Identity: This type of attack involves a malicious device pretending to be a legitimate node in the CRN [10]. While seeming to cooperate with the real nodes in the CRN, the impostor can falsify data to promote greedy spectrum utilization, network failure, network impairment, exclusion of secondary users from certain frequencies, or other malicious goals [3].

4) Unauthorized Use of Media: This category of threat involves malicious users simply transmitting on frequency bands for which they are not authorized to use by the CRN or a regulatory body in order to gain more traffic capacity [3]. This type of attack is aided by the common practice of using contention based MAC protocols in wireless networks. Since these protocols check for active transmissions in a channel before proceeding, nodes that implement them are vulnerable to greedy transmitters that do not observe the protocol [33].

5) Jamming Primary Users: This type of attack is performed by malicious CRN nodes or other agents in order to impair the operation of licensed networks. CRN nodes make excellent vehicles for DoS attacks due their flexible transmission capabilities. These attacks are dangerous to CRNs because they deny secondary users the potential to use a band and regulatory bodies might clamp down on the operations of CRNs to prevent further interference with their paying customers if these attacks become too common [3].

VI. Cognitive Radio Behavior Countermeasures

Section V introduced the two main categories of attacks that exploit CRNs' cognitive behavior: denial of service and greedy attacks. In this section we present solutions from literature for these threats.

A. Denial of Service Attacks

DoS attacks focus on stopping network communication by flooding the utilized spectrum with high power interference. CRN service channels are more resilient to these attacks than traditional radio network channels because CRNs typically implement DSA. In DSA, CRs periodically scan the spectrum for open channels they can communicate on. This behavior avoids jammed service channels with the same mechanism that prevents DSA CRs from interfering with primary users or attempting to communicate on an already occupied band [4].

CRNs rely on sharing sensing data to arrive at a common channel for communication. This sharing typically takes place over a common control channel. In order to combat jamming attacks against that control channel, CRN nodes can implement either of two main actions. The first option is to enact a frequency hopping control channel to avoid jammed frequencies. Unfortunately, this decreases throughput and is vulnerable to jamming if the hopping pattern is discovered by the attacker. The second method is to control the CRN using orthogonal frequency division multiplexing. This spreads out the power spectral density of the signal making it very difficult to jam but may interfere with primary users [3] [7] [10] [29].

One particular DoS attack focuses on jamming whatever frequency band is currently most active. In order to counter these MAB jamming attacks, a CRN can implement a coordinated concealment strategy to hide its real communications. This works by ordering a few secondary nodes to converge on a frequency to create a false MAB while the true activity happens on a separate band with less spectral energy density. This is an effective countermeasure, but it has the drawbacks of expending recourses without directly accomplishing communication, potentially interfering with primary users, and requiring multiple nodes to send a single message [30].

B. Greedy Attacks

Greedy attacks are caused by malignant nodes that try to gain more resources for their own use than they are allocated by a CRN's resource management protocol [31]. The countermeasures for greedy attacks can be generalized to two steps: determining which, if any, entities are behaving greedily and shutting those entities down. If it is not possible for the CRN to disable a greedy node, then it should alert the network's operator to resolve the problem.

There are two common techniques for identifying nodes that are malignantly changing cognitive control messages. The first method is to exclude nodes from the network if their trustworthiness decreases too drastically. Trustworthiness is calculated based on the reputation of each node. Consistently providing other nodes with good sensor information increases a node's trustworthiness, doing the opposite results in the bad node being banished from the network. This is typically accomplished by initially assuming all nodes are honest and only discounting them once a certain threshold value of trustworthiness has been breached as determined by a central authority or consensus algorithm [3] [34] [35]. The other method is to use an authentication server to verify the identity of cognitive control data providers and reject all communications from unauthenticated sources [14].

In order to identify primary user emulators, CRN nodes can analyze the signals coming from suspected primary users [10]. While there are several different analysis techniques that can be implemented to detect these scammers, the most successful of them is based on verifying a primary user's transmission source against a database of primary user locations. This signal source localization is accomplished using the distance difference test to compare the phase of the signal received from a potential primary users at different known node locations [3]. Alternatively, when those primary users are TV stations, AES encrypted IDs could be implanted in the DTV data. CRN nodes could then recognize false primary users by comparing the decrypted data to its expected value [32].

In order to distinguish legitimate CRN nodes from impostors, each node should be authenticated and authorized. One algorithm, the Extensible Authentication Protocol, allows fast radio property changes without the need to consult an authentication, authorization, and accounting server. This protocol's implementation must be topology dependent; if the network is centralized, then a central certification authority should be established, but, if the architecture is distributed, then techniques for authorization such Pretty Good Privacy should be borrowed from mobile ad hoc networks [3] [10].

One approach to combating the unauthorized use of media in CRNs and primary user jamming is to implement the anti-malware techniques in Section IV-C. Alternatively, some researchers have proposed a spectral monitoring program that uses a subset of nodes or a time share on all nodes to monitor the radio spectrum for abusive nodes [3] [36].

VII. Outstanding Challenges

Security is an ever evolving field. New attacks are under contentious development preventing us from reaching a point where it is safe to stop innovating protection practices. In support of this innovation, all the countermeasures described in Sections IV and VI should be periodically reviewed and updated. With this in mind, there are currently several areas of CRN security research that need addressing. First, CRN nodes rely heavily on digital signal processing to operate. SDR hardware fast enough to perform essential CRN functions is expensive in both power and money. The challenge is to reduce the overhead security measures add on top of these core processes [3]. Second, methods for identifying primary user emulators are currently limited to a small number of primary user waveforms such as digital television broadcasts. Research is needed to identify impersonators of a wider variety of waveforms, particularly for protocols that have mobile transceivers [3]. Third, so far most strategies for responding to threats to a CRN have worked primarily with a single level of the communication stack. Further research into cross-layer security strategies is needed to improve threat response in CRNs [10]. Finally, one of the biggest challenges in CRN security is standardization. Before this technology moves from labs to consumers, standards must be in place to ensure user security. Writing these standards is one of the largest present challenges in the field [3].

VIII. Conclusion

Though cognitive radio network security is a maturing field, it requires continuous improvement like all branches of networking security. Security threats tend to focus on two main aspects of CRNs: radio configurability vulnerabilities and cognitive radio behavioral vulnerabilities. Techniques exist to counter many of these threats but some are less than ideal in terms of cost. Accordingly, CRN security is an open research topic that will continue well into the future.

References

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *Selected Areas in Communications, IEEE Journal on*, vol. 23, no. 2, pp. 201–220, Feb 2005.

[2] D. B. Rawat, M. Song, and S. Shetty, *Dynamic Spectrum Access for Wireless Networks*. Springer, 2015.

[3] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 2, pp. 355–379, Second 2012.

[4] M. Song, C. Xin, Y. Zhao, and X. Cheng, "Dynamic spectrum access: from cognitive radio to network radio," *Wireless Communications, IEEE*, vol. 19, no. 1, pp. 23–29, February 2012.

[5] D. B. Rawat, S. Shetty, and C. Xin, "Stackelberg-Game-Based Dynamic Spectrum Access in Heterogeneous Wireless Systems," *IEEE Systems Journal*, in press, Early Access Available: http://dx.doi.org/10.1109/JSYST.2014.2347048.

[6] "Ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: wireless lan medium access control (mac) and physical layer (phy) specifications - redline," *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) - Redline*, pp. 1–5229, March 2012.

[7] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 1, pp. 428–445, First 2013.

[8] J. L. Mauri, K. Z. Ghafoor, D. B. Rawat, and J. M. A. Perez, *Cognitive Networks: Applications and Deployments*. CRC Press, 2014.

[9] D. B. Rawat and D. C. Popescu, "Precoder adaptation and power control for cognitive radios in dynamic spectrum access environments," *Communications, IET*, vol. 6, no. 8, pp. 836–844, 2012.

[10] A. Attar, H. Tang, A. Vasilakos, F. Yu, and V. Leung, "A survey of security challenges in cognitive radio networks: solutions and future research directions," *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec 2012.

[11] R. K. Sharma and D. B. Rawat, "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1023 – 1043, 2015.

[12] D. B. Rawat, S. Shetty, and K. Raza, "Geolocation-aware resource management in cloud computing-based cognitive radio networks," *International Journal of cloud computing*, vol. 3, no. 3, pp. 267–287, 2014.

[13] D. Welch and S. Lathrop, "Wireless security threat taxonomy," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, June 2003, pp. 76–83.

[14] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *Network, IEEE*, vol. 27, no. 3, pp. 28–33, May 2013.

[15] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE*, vol. 19, no. 6, pp. 106–112, December 2012.

[16] Y. Kondareddy, P. Agrawal, and K. Sivalingam, "Cognitive radio network setup without a common control channel," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, Nov 2008, pp. 1–6.

[17] K. Sakaguchi, F. Chih, T. D. Doan, M. Togooch, J.-i. Takada, and K. Araki, "Acu and rsm based radio spectrum management for realization of flexible software defined radio world," *IEICE transactions on communications*, vol. 86, no. 12, pp. 3417–3424, 2003.

[18] C. Li, A. Raghunathan, and N. K. Jha, "An architecture for secure software defined radio," in *Proceedings of the Conference on Design, Automation and Test in Europe*, ser. DATE '09. 3001 Leuven, Belgium, Belgium: European Design and Automation Association, 2009, pp. 448–453.

[19] M. Beller, L.-F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *Selected Areas in Communications, IEEE Journal on*, vol. 11, no. 6, pp. 821–829, Aug 1993.

[20] G. Singh and A. Supriya, "A study of encryption algorithms (rsa, des, 3des and aes) for information security," *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33–38, 2013.

[21] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *Communications, IET*, vol. 6, no. 16, pp. 2676–2687, November 2012.

[22] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *Communications, IEEE Transactions on*, vol. 61, no. 12, pp. 5103–5113, December 2013.

[23] H. Zhao, H. Liu, Y. Liu, C. Tang, and G. Pan, "Physical layer security of maximal ratio combining in underlay cognitive radio unit over rayleigh fading channels," in *Communication Software and Networks (ICCSN), 2015 IEEE International Conference on*, June 2015, pp. 201–205.

[24] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: from cognitive radio miso channels to secrecy miso channels," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, Nov 2009, pp. 1–5.

[25] Y. Pei, Y.-C. Liang, L. Zhang, K. Teh, and K. H. Li, "Secure communication over miso cognitive radio channels," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 4, pp. 1494–1502, April 2010.

[26] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *Communications, IEEE Transactions on*, vol. 58, no. 6, pp. 1877–1886, June 2010.

[27] A. Brawerman, D. Blough, and B. Bing, "Securing the download of radio configuration files for software defined radio devices," in *Proceedings of the Second International Workshop on Mobility Management &Amp; Wireless Access Protocols*, ser. MobiWac '04. New York, NY, USA: ACM, 2004, pp. 98–105.

[28] E. Gallery and C. Mitchell, "Trusted computing technologies and their use in the provision of high assurance sdr platforms," in *2006 Software Defined Radio Technical Conf. Product Exposition*, 2006.

[29] M. Jo, L. Han, D. Kim, and H. In, "Selfish attacks and detection in cognitive radio ad-hoc networks," *Network, IEEE*, vol. 27, no. 3, pp. 46–50, May 2013.

[30] N. Hu, Y.-D. Yao, and J. Mitola, "Most active band (mab) attack and countermeasures in a cognitive radio network," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 3, pp. 898–902, March 2012.

[31] L. Zhu and H. Zhou, "Two types of attacks against cognitive radio network mac protocols," in *Computer Science and Software Engineering, 2008 International Conference on*, vol. 4, Dec 2008, pp. 1110–1113.

[32] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 5, pp. 772–781, May 2014.

[33] O. Queseth, "Cooperative and selfish behavior in unlicensed spectrum using the csma/ca protocol," in *Proc. Nordic Radio Symposium*, 2004, pp. 404–408.

[34] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference on*, March 2009, pp. 130–134.

[35] ——, "Catchit: detect malicious nodes in collaborative spectrum sensing," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, Nov 2009, pp. 1–6.

[36] G. Atia, A. Sahai, and V. Saligrama, "Spectrum enforcement and liability assignment in cognitive radio systems," in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, Oct 2008, pp. 1–12.