A Survey of Security Issues in Cognitive Radio Networks

LI Jianwu[1]*, FENG Zebing[2], FENG Zhiyong[2], ZHANG Ping[1]

[1] Network Information Processing Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Key Laboratory of Universal Wireless Communications Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: In the last decade, cognitive radio (CR) has emerged as a major next generation wireless networking technology, which is the most promising candidate solution to solve the spectrum scarcity and improve the spectrum utilization. However, there exist enormous challenges for the open and random access environment of CRNs, where the unlicensed secondary users (SUs) can use the channels that are not currently used by the licensed primary users (PUs) via spectrum-sensing technology. Because of this access method, some malicious users may access the cognitive network arbitrarily and launch some special attacks, such as primary user emulation attack, falsifying data or denial of service attack, which will cause serious damage to the cognitive radio network. In addition to the specific security threats of cognitive network, CRNs also face up to the conventional security threats, such as eavesdropping, tampering, imitation, forgery, and noncooperation etc.. Hence, Cognitive radio networks have much more risks than traditional wireless networks with its special network model. In this paper, we considered the security threats from passive and active attacks. Firstly, the PHY layer security is presented in the view of passive attacks, and it is a compelling idea of using the physical properties of the radio channel to help provide secure wireless communications. Moreover, malicious user detection is introduced in the view of active attacks by means of the signal detection techniques to decrease the interference and the probabilities of false alarm and missed detection. Finally, we discuss the general countermeasures of security threats in three phases. In particular, we discuss the far reaching effect of defensive strategy against attacks in CRNs.

Keywords: CRNs security; physical layer security; security capacity; active attacks; passive attacks

I. INTRODUCTION

Growing business demands have driven wireless communication technology renewal and evolved in a rapid pace. Hence, the limited spectrum resource contradicts with the growing business demands. The report of Federal Communications Commission (FCC) mentions that currently spectrum scarcity is largely due to the inefficient and rigid regulations rather than the physical shortage of the spectrum [1]. Recently, Cognitive Radio Network (CRN) has been brought to the forefront to solve the conflict between limited spectrum supply and spectrum demand from ever-increasing wireless applications and services. CRN is defined as a wireless network employing technology to obtain the knowledge of its operational and

This paper analyzes the security issues in cognitive radio networks and investigates the most important contributions on security threats and the current state of the art techniques.

geographical environment, established policies and its internal state, thus to dynamically and autonomously adjust its operational parameters and protocols according to the obtained knowledge in order to achieve end-to-end network optimization [2].

However, CRNs work in an open and random access networks environment, where the unlicensed Secondary Users (SUs) can use the channels that are not currently used by the licensed primary users (PUs) by spectrum-sensing technology [3][4]. Cognitive users (the terms "secondary users" and "cognitive users" are used interchangeably unless explicitly mentioned) have flexible and convenient channel access mode, which greatly improves the efficiency of spectrum utilization, and effectively solves the problem of spectrum shortage.

The security of cognitive radio network has been attracting growing attentions. Because various unknown wireless devices are allowed to opportunistically access the licensed spectrum in the architecture of cognitive radio, cognitive radio systems are vulnerable to malicious attacks. Besides, CRNs not only face all the security threats in traditional wireless networks, such as eavesdropping, tampering, imitation, forgery, and noncooperation etc., but also new security threats related to unique cognitive characteristics, such as primary user emulation attack, falsifying data, denial of service attack etc.. At present, the research on network security has gradually become one of the hottest topics of cognitive radio networks. Therefore, it is necessary to survey the research status of security techniques for cognitive radio networks.

This paper investigates the current studies of security issues in cognitive radio networks, and addresses identified challenges with a particular research area. We look forward to introduce the current research hot-point and guide for the future research. The main thrust of contents is how to guarantee the wireless network security, furthermore to improve the utilization rate of spectrum resources and increase the achievable system capacity. It is known that cognitive radio technology can effectively improve the capacity of wireless networks. However, the existence of malicious nodes is a great menace for improving the capacity, which can be classified into two basic types [5] *passive attacks* and *active attacks*.

- *An active attack* corresponds to the situation in which a malicious user intentionally disrupts the system.
- *A passive attack* corresponds to the situation in which a malicious user attempts to interpret source information without injecting any information or trying to modify the information; i.e., passive attackers listen to the transmission without modifying it.

On the whole, we firstly introduce the active attack and its countermeasures from the view point of signal detection and estimation. Then we introduce the defensive strategy of passive attack from the perspective of the information theory. The overall goal is to ensure the network security and enhance the network capacity. Therefore, the remains of this paper are organized as follows. Section II describes the active attack and defensive strategy in different category. In Section III, secrecy capacity will be analyzed from the perspective of passive attack. Next, Section IV presents the future research aspects. Finally, we provide some concluding remarks in Section V.

II. The Active Attacks and Defensive Strategy

To ensure the security and improve the capacity of CRNs, the key technique is intrusion detection that achieves an accurate decision of active attack users and provides a support of effective management of attackers follow-up. In cognitive radio networks, the intrusion detection (or attack detection) is a very important phase in the counteracting network security. In this section, we will give an overview of the attack detection that has been studied on the security threats and countermeasures in the past few years. Before the introduction, it is necessary to give a brief description of the spectrum detection or primary user detection,

which is the premise of a cognitive user to access the networks. Based on the spectrum sensing, a large number of detection methods against the attacks are proposed. Moreover, we will present the different categories of attacks based on the destructiveness and give the defense methods against the attacks followed in each category. At last, the whole countermeasures for security threats are provided.

2.1 Intelligent spectrum sensing

Security issues in CRNs have become unavoidable challenges, and how to solve the security problems has become a research hotspot. In [6], Fragkiadakis et al. have given a comprehensive survey of the existing works on CRN security, which introduced various security threats and detection techniques in detail. Security threats are mainly related to two fundamental characteristics of cognitive radios: cognitive capability, and reconfigurability. Threats related to the cognitive capability include attacks launched by adversaries that mimic primary transmitters, and transmission of false observations related to spectrum sensing. Hence, the key technology to deal with security threats is spectrum sensing (detection), including Primary User detection and Attack User (or named as attacker) detection. Once the primary user signal is detected accurately, it provides a way to differentiate the attacker signal from it. Primary user signals can be identified accurately by studying their signal characteristics [7].

In the past few years, a large number of spectrum sensing methods are proposed for detecting the presence of transmitted signal and identifying the signal type. There we will introduce three main types in the following, and more in-depth research can be referred to [8].

2.1.1 Energy detection

Energy Detection, also known as radiometry or periodogram, is the most common method of signal detection, which has low computational and implementation complexities [8]. It does not require prior knowledge of the primary user' signal, and not need special designs for detecting spread spectrum signals [9]. Based on a comparison between the output of the energy detector and the given threshold for primary users, the challenges for energy detection are the selection of the appropriate detection threshold, the inability to differentiate interference from primary user's signal and noise, and the poor performance under low signal-to-noise ratio (SNR) values [10]. There has been abundant research on these challenges, such as [11][12]. The typical structure of energy detector is shown in Fig. 1.

The performance analysis of energy detection

- **Advantages** Energy detection is the most widely method used because of its simplicity and low computational overhead.
- **Disadvantages** The most vulnerable aspect is that it does not perform well in low SNR environments.

2.1.2 Feature detection

Feature detection derives from the specific features associated with the modulated signals transmitted by primary users. In many cases, signals have periodic statistic features such as modulation rate and carrier frequency which are usually viewed as cyclostationary characteristics. In detection, the cyclostationary characteristic of a primary user's signal can be distinguished from noise in its statistical properties such as its mean and autocorrelation [13][14]. Compared with energy detection, cyclostationary detection is not sensitive to noise uncertainty, so it has better robustness in low SNR regimes. However, this method requires more prior information on the primary user signals to decide the occupancy of primary users. As the consequence, feature detection has much greater complexity [15][16]. The typical

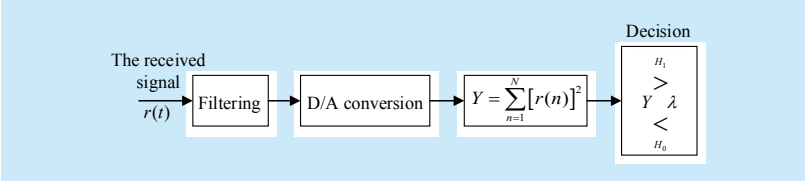

Fig.1 *The structure and the executive process of energy detector*

structure of cyclostationary detector is shown in Fig. 2.

The performance analysis of feature detection:

- **Advantages:** The cyclostationarity detection can differentiate noise from primary users' signals, and can be used to distinguish the different types of transmissions and primary users effectively.
- **Disadvantages:** The main drawback of the cyclostationarity characteristic is its computational complexity for its implementation.

2.1.3 Matched filter and waveform-based detection

Matched filter detection is an optimized detection method on the basis that the primary user's signal as prior knowledge for the secondary users. The advantage of the matched filter detection is the short time to achieve a certain probability of a false alarm or probability of a misdetection. The matched filter has a requirement of fewer signal samples, which grows as for a target probability of false alarm at low SNRs [[17, 18]. Thus, there exists a SNR wall for a matched filtering method [19]. Moreover, matched filter detection requires that the received signals are demodulated. Perfect knowledge of the primary users signal is required, so the implementation complexity of a sensing unit is high impractically [20]. To solve the problem of SNR wall, waveform-based detection is proposed to improve the performance of match filtering detection when the number of samples is large enough [21]. However, information on the patterns of the primary user's signal is a prerequisite for implementing waveform-based detection, so minimizing the implementation complexity is still an open issue. The typical structure of matched filter detector is shown in Fig. 3.

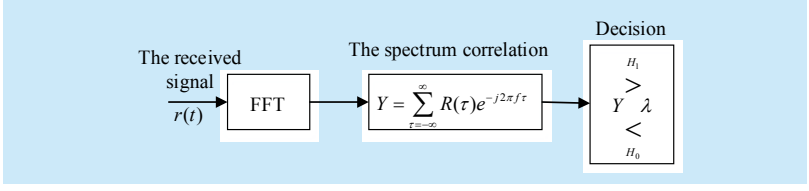

Fig.2 *The structure and the executive process of cyclostationary feature detector*

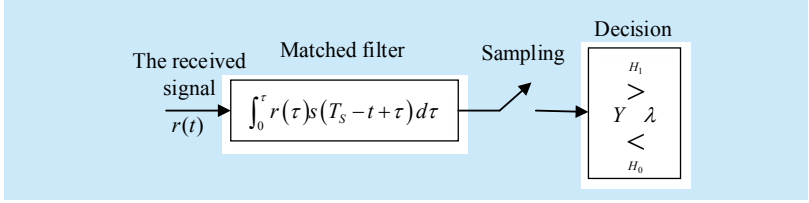

Fig.3 *The structure and the executive process of matched filter detector*

The performance analysis of matched filter detection:

- **Advantages:** It is the optimum method for detection when the transmitted signal is known. The main advantage of matched filtering is the short time to achieve a certain probability of false alarm or probability of missed detection compared to other methods.
- **Disadvantages:** It requires perfect knowledge of the primary users signaling features such as bandwidth, operating frequency, modulation type and order, pulse shaping, and frame format, etc..

2.2 The classifications and presenting solutions of attacks

In section 2.1, we mainly introduce the primary user detection methods, that is, a secondary user can use different methods to sense the presence of the primary user in the spectrum, such as energy detection, matched filter detection and cyclostationary feature detection [22]. However, the most suitable technique is energy detection for detecting attack users. First, the energy detection method is most widely used and can be easily implemented. Second, an intelligent attacker can potentially generate a signal with the features similar to those of the primary user, such as modulation schemes and cyclostationary characteristics. Hence, a secondary user cannot distinguish the attacker and the primary user based only on matched filter and cyclostationary spectrum sensing methods. Furthermore, different attacks have different fundamental characteristics, and they can be classified into three categories [23] in the light of harmful levels of consciousness and subjective attack in CRNs, as shown in Tables 1, 2 and 3. Behind each kind of attacks,

there is corresponding detection methods followed.

2.2.1 Malicious users

Malicious users are actively to destroy the networks rather than their own occupation (or utilization). These types' attacks mainly include: *Primary Users Emulation Attacks* (PUEA) that mimic incumbent signals in order to cause *Denial of Service* (DoS) attacks, especially in distributed networks. They can cooperate and transmit to fake incumbent signals, thus making a cognitive user hop from band to band and severely disrupting its operation. *Spectrum Sensing Data Falsification attacks* (SSDF) sends false observations in order to confuse other nodes or the Fusion Center (FC), and their aims are to lead FC or other users to falsely conclude that there is or not an ongoing incumbent transmission. *Congestion Attacks* is the attack type where attackers flood Common Control Channel (CCC) in order to cause an extended DoS attack. *Jamming Attacks* is the attack type where attackers cause DoS attacks at the physical layer by creating interference.

Most of the contributions regarding security propose appropriate techniques for the detection of malicious users, with no modification of the incumbent signal is necessary. Furthermore, a few contributions assuming that the location of the primary transmitters is known.

Chen et al., in [24], utilize both the location information of the primary transmitter and the Received Signal Strength (RSS) characteristics. This approach consists of three phases: (i) *verification of signal characteristics*, (ii) *received signal energy estimation*, and (iii) *localization of the transmitter*. It mainly focuses on the localization of the transmitter using a method based on RSS measurements collected by a cognitive radio network.

In [25][26], using analytical models for the received power for attack detection, Z. Jin et al. propose the Fenton's approximation and Wald's Sequential Probability Ratio Test (WSPRT) to analyze the received power. Cognitive users measure the received signal including power, modulation mode, location etc. and give a decision according to the preset threshold on whether the detected signal is sent by a legitimate primary transmitter or an illegal attacker.

Table I *The classifications and presenting solutions of malicious attacks*

Attack types	Counterchar-acteristics	Countermeasures & Contributions	Whether cooperation
PUEA	Using location analytical models for the received power for attack detection.	Fenton's approximation and Wald's Sequential Probability Ratio Test (WSPRT) [25], [26]	No
		Distance Ratio Test and Distance Difference Test (DRT&DDT) [24] [27]	No
		Fenton's approximation and Markov Inequality [29]	Yes
		Time Difference of arrival (TDOA) and Frequency Difference of arrival (FDOA) [30]	No
SSDF	Using the adjacent helper nodes for attack detection	Collaborative spectrum sensing technique [31] [32] [33] [34] [35]	Yes
		Social network [37],[38]	Yes
		Neighbor Assisted Distributed Spectrum decision (NEAT) [39] [40]	Yes
		Using cooperative sensing scheme [41]	Yes
Other attacks	Application layer management mechanism	Intrusion Detection System (IDS) [42] [43], [44]	No
		Transmitter fingerprinting [45]	No

The variance detection method is proposed in [27]. In this work, Chen et al. consider that attackers have variable transmit power and adapt it so as to effectively jam the target network. Using the defense strategy of variance detection method can get an effective defense against PUEAs.

Considering the locations of primary users are not static sometimes, Liu et al., in [28], state that the channel impulse response can be used to determine whether a primary transmitter changes its location. It needs using the adjacent helper nodes for attack detection. This node is called as a bridge enabling SUs to verify cryptographic signatures carried by the helper node's signals, and then obtain the helper node's link signatures in order to verify the primary transmitter's signals.

In [29], Anand et al. propose an analytical approach based on Fenton's approximation and Markov inequality and obtain a lower

Table II *The classifications and presenting solutions of greedy attacks*

Attack types	Countercharacteristics	Countermeasures & Contributions	Whether cooperation
PUEA	Using reputation metric and fusion rules.	Metric method based on reputation [46]	No
		Using WSPRT for assigning weights [47] [48]	No
		Distributed Consensus Algorithm [50]	No
		Dempster-Shafer theory of evidence [51] [52]	No
	Using location analytical models for the received power for attack detection.	Enhanced-WSPRT (EWSPRT) algorithm [49]	No
		The Received Signal Strength (RRS) [53]	Yes
		Double-Sided Neighbor Distance (DSND) algorithm [54]	Yes
SSDF	Using collaborative detection methods	Kernel KMC (K-Means Clustering) Method [55];	Yes
		Joint Spatio-temporal Joint Spatio-temporal Spectrum Sensing algorithm based on three-phase [56]	Yes
		Conditional Frequency Check (CFC) statistic based on the Markovian model [57]	Yes

Table III *The classifications and presenting solutions of unintentional attacks*

Attack types	Countercharacteristics	Countermeasures & Contributions Whether cooperation
Unintentional attacks	Hardware-based protection schemes	Using Secure Radio Middleware (SRM) [58], [59];
		Using characteristics of FPGAs [62];
	Software-based protection schemes	Tamper resistance [60];
		Light Secure Socket Layer (LSSL) protocol [61];
	Other protection schemes	Employing biometric sensors and processors for authentication [63]

bound on the probability of a successful attack on a secondary user by a set of co-operating malicious users. They consider a fading wireless environment and discuss the various parameters that can affect the feasibility of the attack that is the first analytical treatment to study.

In [30], a semi range-based localization algorithm is proposed to estimate the positions of the PUs. The basic idea is to take advantage of the estimated detection probabilities, which can be obtained from the binary detection indicators of the SUs, and to estimate the distances between themselves and the PUs. Moreover, they introduce both a weighted least-squares method and an iterative procedure in order to improve the accuracy of the localization algorithm.

A solution to malicious users is the collaborative spectrum sensing technique [31-35] where a number of users sense the environment and share their observations. This technology has two types: the distributed and centralized. In centralized model, the FC fuses the provided information taking the final decision regarding the presence or absent of incumbent transmissions. And in distributed model, each SU makes its decision not only based on its observations but also on observations shared by other SUs [36].

A key feature of cognitive radio network is the intelligence of secondary users who can collaborate to improve the system security performance [37]. In [38], the social behavior is studied in cognitive radio networks using analysis tools in social networks. Li et al. proposes a recommendation system for cognitive radio, thus incurring the channel preference propagation in the corresponding random geometric network. For cognitive radio networks having a grid topology, the ergodicity of the dynamics is studied using the model of interacting particles in nonequilibrium statistical mechanics. A mean field based ordinary differential equation is used to describe the dynamics of the channel preference propagation.

In [39][40], Jin et al. propose a robust spectrum decision protocol neighbor assisted spectrum decision protocol (NEAT) using individual spectrum decisions made by secondary nodes, which is resilient to PUEA in CRNs. In order to enable each secondary node to make an individual spectrum decision, they characterize the received power at good secondary user firstly by means of a flexible log-normal sum approximation. The received power characteristic is used to determine the probability of successful PUEA on each secondary user, which is used to develop the proposed protocol.

In [41], Kaligineedi et al. propose a scheme to identify the malicious users in a cooperative

sensing system employing energy detection, which is based on the non-parametric outlier detection techniques. Considering partial information of the PU activity, they also propose a cooperation-based malicious user detection scheme by using spatial information.

In cognitive radio networks, any kind of intrusions should be detected before attackers can harm the network (i.e., cognitive nodes) and/or information fusion center. Intrusion Detection Systems (IDSs) are proposed for wireless network security. Intrusion detection systems (IDSs) perform: monitoring audit data, looking for intrusions to the system, and initiating a proper response. As such, there is a need to complement traditional security mechanisms with efficient intrusion detection and response [42]. In [43][44], there are some new detection schemes present, such as *agent based distributed and collaborative IDSs*, *clustering (hierarchical) based IDSs, statistical detection based IDSs, misuse detection based IDS, reputation (trust) based IDSs, zone based IDS, game theory based IDSs, genetic algorithm based IDS*, and some others.

Furthermore, the fingerprinting is one of the important means of identification. A lot of radio identifications are also using "fingerprints" of signals, such as the type of modulation, difference in accuracy of carrier frequency and in spurious output, the signal bandwidth, transfer rate and so on. However, some of these parameters, such as modulation type, signal bandwidth and information transfer rate can be copied easily, which have weak defense against PUE attacks. In [45], Zhao et al. propose the approach that erases the modulation to get the carrier with phase noise which is random for each transmitter but unique. This approach named fingerprinting that identifies the transmitter according to uniqueness feature of the phase noise of Local Oscillator, in order to distinguish the legitimate primary users from the emulated ones. In the experiments, using fingerprinting as the basis of transmitter identification to defend PUE attack can obtain a good performance.

2.2.2 Greedy users

Greedy users launch attack actively in order to maximize their own interests, including PUEA that by transmitting fake incumbent signals force all other users to vacate a specific band (spectrum hole) to acquire its exclusive use and SSDFA that continuously report that a specific spectrum hole is occupied by incumbent signals. The goal of these users is to monopolize the specific band by forcing all other users to evacuate it. In attack detection, there is no clear distinction between malicious users and greedy users generally.

In cognitive radio networks, a greedy or malicious user can modify its air interface to mimic a primary user. Hence, it can mislead the spectrum sensing performed by legitimate primary users. There is no significant difference for the detection of greedy users and malicious users, although they are classified into two different categories.

Fadlullah et al., in [46], propose a metric method based on reputation to detect and isolate attackers from legitimate SUs. By computing the reputation of each user, FC makes the decision that the smaller the reputation metric is, the more reliable the user is. If the reputation metric of a user exceeds a predefined threshold, its decisions are isolated and not used by the FC.

In [47], Chen et al. use the WSPRT to assign weights to each SU. If the output of each SU is the same with the output produced by FC, the reputation metric of the user is incremented by one, otherwise, it is decremented. The same as in [48], if the node temporarily misbehaves, its reputation metric can be restored after a few samples and it starts behaving correctly again.

Zhu et al. argue that there are several drawbacks although WSPRT is a robust method against SSDF attacks in [49], and propose the Enhanced–WSPRT (EWSPRT) algorithm in [47], which has several modifications/improvements compared to WSPRT. The latter method proposed is the Enhanced Weighted Sequential Zero/One Test (EWSZOT). This

method does not use sequential test like EWSPRT. It collects samples one-by-one and the test is terminated if the reported value is larger than pre-defined thresholds. The three algorithms, namely, WSPRT, EWSPRT and EWSZOT, are evaluated by using simulations in different testing indexes.

Yu et al. propose a scheme to defend against SSDF attacks in a distributed model, where SUs exchange information and decide independently upon the presence of incumbent transmissions [50]. Each SU applies energy detection to detect the presence of a primary receiver, and then it updates its measurements from similar information received by its neighbors and sends back the updated information.

In [51], N. Nhan and I. Koo isolate outliers by using a reputation scheme based on the Dempster-Shafer theory of evidence [52]. A reputation metric is assigned to each SU based on the difference between its output and the final verdict produced by the FC and the metric is used as a weight for the Dempster-Shafer algorithm.

An anomaly-based detection method using statistics is described in [53]. A grid of sensors, which are divided into clusters, send information of their received power (RSS) along with their location to the FC.

In [54], a Double-Sided Neighbor Distance (DSND) algorithm is proposed for the detection of outliers. The authors study two attack modes, i.e., the independent attack where an adversary does not know the reports of the legitimate nodes and the dependent attack where it is aware of what other nodes report.

Ding et al., in [55], provide a novel effective algorithm that use Kernel KMC (K-Means Clustering) method to be answerable for attacker detection, which not only improves the attacker detection performance but also offers processing and memory savings.

In order to improve the cooperative detection performance, Ding et al., in [56], design a joint spatio-temporal spectrum sensing algorithm based on three-phase (i.e., a global cooperation phase, a local cooperation phase and a joint decision phase).

Based on the Markovian models that characterize the spectrum state behavior more precisely [57], He et al. propose an attacker detection method using conditional frequency check (CFC) statistics. With the assistance of one trusted user, the proposed method can achieve high malicious user detection accuracy for arbitrary percentage of attackers that may even be equipped with more advanced sensing devices and can thus improve the collaborative spectrum sensing performance significantly.

2.2.3 Unintentionally misbehaving users

Unintentionally misbehaving users that report faulty observations for spectrum availability, not because they are malicious or greedy, but parts of their software or hardware are malfunctioning. The reason for this can be a random fault or a virus [58-60].

In [59], Li et al. propose the usage of Secure Radio Middleware (SRM) layer, which is purely implemented in software and resides between the operating system and the hardware. Its role is to check all software requests sent to the hardware layer for operations regarding transmission power, frequency, type of modulation, etc.. All requests are checked against a policy database, and non-conforming requests are discarded. Security policies can be provided by dedicated policy servers by other SUs or primary transmitters.

Brawerman et al., in [61], propose the Light Secure Socket Layer (LSSL) protocol that securely connects SDR devices with software servers maintained by the manufacturers, which are suitable for resource-constraint devices for requiring less bandwidth than SSL.

In [62], Uchikawa et al. describe a secure downloading system that uses the characteristics of FPGAs hosted in a SDR. The connections between the configuration logic blocks (fundamental units of FPGAs) can be arranged in many ways, enabling high security encipherment. The authors show that their proposed scheme has high immunity against illegal acquisition of soft-ware through replay attacks.

Campbell et al., in [63], highlight the im-

portance of user authentication in a SDR system. They propose a security architecture that can employ biometric sensors and processors for authentication based on users' traits such as voice, fingerprint, etc..

2.3 A summary of countermeasures for security threats

In this section, some critical issues of CRNs in three types of active attack were surveyed. The best defensive strategy is offense, that is, active signal detection against attack effectively. In the above attack detections, most of them are based on the detection probability as the measurable indicators, e.g., false alarm probability P_f and missed detection probability P_m, although different methods defense different type of attack.

III. The Passive Attack and Defensive Strategy

In addition to the active attack, such as PUEA, SSDF and DoS attack, an eavesdropper as the passive attack is considered in the security of CRNs, which attempts to intercept the legitimate transmissions. However, it is typically undetectable since the eavesdropper keeps silent without transmitting any active signals. Traditionally, security has been a higher layer issue, usually handled by encryption. And this is usually handled at the application layer or just below at the presentation layer. However, the encryption can be difficult to manage without infrastructure. That is, in a peer-to-peer network such as an ad hoc network, or cognitive radio network, key management becomes more and more complicated as the number of nodes increases [64]. Physical (PHY) layer security approaches for wireless communications can prevent eavesdropping without upper layer data encryption. Hence, it is more suitable using the physical properties of the radio channel to help secure CRNs. Recent years, PHY layer security for cognitive radio networks has attracted the attention of scholars, in [65] and [66]. In this section, we will briefly introduce the development of the PHY layer security in the view of information theoretic and analyze the issues of security capacity in CRNs. Moreover, the information theoretic security is introduced detailed and the principal results in this area are reviewed, the researchers who want to further study this topic can refer to [5].

3.1 The PHY layer security

This work was pioneered by Shannon in [67], and he firstly proposed the conception of information-theoretic security in his classical dissertation, which has proven that there is an optimal secure communication system that needs encryption of one-word-one-key. In other words, how many codes are transmitted as the passwords are required. Hence, this system is an ideal secure communication system. However, it is difficult to achieve because managing password is too large and this perfect secrecy communication way is only a vision theory for a very long time.

Based on the Shannon's information-theoretic security, Wyner [68] proved the definition of secrecy capacity. If the eavesdropper channel quality is worse than the legitimate receiver, one can always find a channel coding, with the case of correct demodulation in the legitimate users, the eavesdropper cannot obtained any information from the received signal, and the communication system achieves the perfect secrecy.

Note that it is often assumed that the channel state information (CSI) is known at both the transmitter and the receivers during each symbol time. The CSI at the transmitter can be realized by a reliable feedback from the two receivers, who are participants in the network and are supposed to receive information from the transmitter. Based on the CSI, the transmitter can dynamically change its transmission power to achieve good performance. Henceforth, throughout the paper, we assume that the CSI of transmitter is perfect unless specific statement.

There is an upper limitation of the rate of such coding mode and Wyner defined this supremum as Secrecy Capacity (encryption ca-

pacity). It will provide security enhancements or standalone security solutions to a host of applications by utilizing secrecy codes technique. This secure communication method actually achieves perfect secrecy communication proposed by Shannon.

The proposed wiretap model is shown in Fig. 4, it is assumed that the signal received by the eavesdropper is a degraded version of the signal received by the legitimate receiver. Accounting for the compromise between the transmission error rate and the security of the transmitted message, Wyner showed that it is possible to implement secure communication. In the later related research, the secrecy capacity C_S is the capacity Legitimate channel C_M minus the capacity of Wiretap channel C_E in addition Gauss noise channel, as shown in formula (1).

$$C_S=C_M-C_E \quad (1)$$

I. Csiszar et al. and S. K. Leung et al. extend the research from the composite (main wiretap) channel to a single-input two-output broadcast channel [69] and to Gaussian channels [70] respectively, and prove that a non-zero secrecy capacity is achievable as long as the main channel is better than the wiretap channel, as shown in Fig. 5.

Later，I. Csiszar et al. further develop the broadcast channel 'wire-tapper' model to the multi-terminal wiretap model, and prove the multi-terminal secrecy capacity [71]. Naturally, in this model, each terminal must have access to some sort of information that can be used to generate a suitable key. In the model considered here, the way in which this information shared determines the level of secrecy obtained.

More recently, the impact of channel fading on the secrecy capacity was studied in [72]. The authors point out that the secure communication is feasible over quasi-static fading channel with one eavesdropper, even if the main channel is worse than the wiretap channel on the average. And in [73], Gopala et al. study how to maximize the secrecy capacity and derived the optimal power allocation policies under different assumptions at the transmitter. The secrecy capacity has also been extended into multiple access channels [74] and broadcasting channels [75]. Han et al. in [76] propose an auction theory approach that can improve the secrecy capacity effectively using friendly jammers to introduce extra interference to the eavesdroppers. In [77], the relay–eavesdropper channel model is studied and the authors propose several cooperation strategies and obtain the corresponding achievable capacity bounds. Dong et al. propose the cooperating relays scheme in [78], which is a method to overcome the fragile channel and improve the performance of secure wireless network.

Moreover, in [79], Hong et al. propose the enhancing physical-layer technology in the multi-antenna wireless communication systems. One is the Artificial Noise (AN) that used on top of beam-formed or pre-coded signals to further reduce the reception quality at the eavesdropper. Besides, the AN can be extended to relay system where additional spatial degrees of freedom are provided by the antennas at the relays, which not only can help forward data to the destination but also can emit AN or jamming signals to disrupt the reception at the eavesdropper. Moreover, the authors considered that it is important to study the impact of these secrecy-based physical layer transmission schemes on modern com-

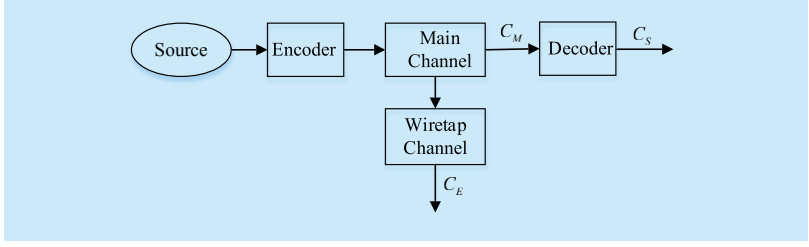

Fig.4 *Wyner's wiretap model*

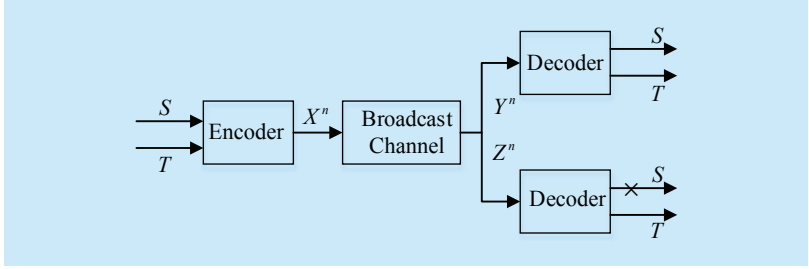

Fig.5 *Csiszar and Korner's wiretap channel model*

munication systems such as cognitive radio and ad hoc networks.

H. V. Poor in [64]is fascinated by the wireless physical layer for improving capacity and reliability. In his work, four physical layer communication problems have been considered and each of them is motivated by considerations at the application layer, namely, issues of information transfer and/or inference. The first of these four problems is physical layer security in wireless communication networks. The second is distributed learning. The third is finite-blocklength capacity, and the fourth is message delivery in small-world networks. The work shows that it is more suitable using the physical properties of the radio channel to help provide secure in CRNs.

However, the forementioned PHY security is the most considered topic in traditional wireless networks, and the same secrecy capacity issues will be faced in cognitive radio networks. The earliest literature that attempts to compute the secrecy capacity of a cognitive network is [80] to the best of our knowledge, where S. Anand and R. Chandramouli compute the primary exclusive region (PER) and the secrecy capacity at a primary receiver in a cognitive radio network.

In that paper, S. Anand and R. Chandramouli extend the approach by Vu et al. in [81] to first obtain the PER (primary exclusive region) of cognitive radio networks operating on a fading wireless channel. And extend the expressions obtained in [82] to obtain the secrecy capacity of a fading cognitive radio network. However, the secrecy capacity of the primary receiver also has the same representation as formula (1), i.e., the original model of security capacity is taking into account in cognitive radio networks.

In [65], Zou et al. consider the physical-layer security against eavesdropping attacks in the cognitive radio network and propose the user scheduling scheme and the artificial noise approach to achieve multiuser diversity for improving the security level of cognitive transmissions with a primary quality of service (QoS) constraint. In this paper, the author derive the closed-form intercept probability expressions of the multiuser scheduling and the artificial noise schemes, and obtain the optimal achievable secrecy rate and intercept probability in Rayleigh fading environments. By exploiting multiuser scheduling, they get an excellent performance for enhancing the cognitive transmission security against eavesdropping attacks.

In [83], Peng et al. present the capacity formulation, which considered the influences of missed detection and false alarm that jeopardize the network throughput (sum capacity). Taking all the elements of cognitive environment into account, the averaged capacities of primary and cognitive link rates can be formulated as follows.

$$\begin{cases} C_p = E\{\Pr(H_1|H_1,\gamma)\lambda E[\log_2(1+\frac{P_p}{\sigma_w^2})] \\ \quad + \Pr(H_0|H_1,\gamma)\lambda E[\log_2(1+\frac{P_p}{\sigma_w^2+I_{pc}})]\} \\ C_c = E\{\Pr(H_0|H_0)(1-\lambda)E[\log_2(1+\frac{P_c}{\sigma_w^2})] \\ \quad + \Pr(H_0|H_1)\lambda E[\log_2(1+\frac{P_c}{\sigma_w^2+I_{cp}})]\} \end{cases} \tag{2}$$

where P_p and P_c are the random received signal power at the primary and secondary receiver, I_{pc} and I_{cp} are the corresponding random interference power, σ_w^2 is the noise power.λ is the transmission probability of the primary user, γ is the sensing threshold, and $\Pr(H_0|H_1,\gamma)$ is the miss-detection probability The secondary transmitter makes a decision to transmit while the primary transmitter is always active. The innermost expectation is performed over fading.

In [84], M. G. Khoshkholgh et al. also present the total secondary service achievable capacity in fading environment with *Overlay*, *Underlay* and *Mixed deployment* respectively. Considering malicious nodes (belong to secondary user and have all the properties of the secondary users), the capacity is closely related to detection probability that the spectrum is available or not.

Furthermore, in [85], Shu et al. have analyzed the impact of interference on secrecy

capacity, and derived the secrecy capacity of the primary link as follows.

$$C_s(x_i, x_j) = \max\{\log_2(1 + \frac{P_{rx}(x_i, x_j)}{W_p + I_p}) - \log_2(1 + \frac{P_{rx}(x_i, e)}{W_e + I_e}), 0\} \quad (3)$$

where (x_i, x_j) means from node x_i to node x_j, (x_i, e) means from node x_i to eavesdropper node, $P_{rx}(x_i, x_j) = \frac{P|h(x_i, x_j)|^2}{d_{i,j}^{\alpha}}$ and P is the transmit power of the primary nodes. $h(x_i, x_j)$ is the complex fading coefficient of the primary link $\overrightarrow{x_i x_j}$, which is assumed constant during the communication interval, $d_{ij} = \|x_i - x_j\|$ is the distance between node x_i and node x_j, and α is the path loss exponent of medium, which varies from 0.8 to 4 due to different communication environment [86]. W_p is the noise power, introduced by the primary receivers and $I_p = \sum_{i=1}^{n} P_s / d_{p,i}^{\alpha}$ is the interference powers of the primary receiver from the cognitive users, where n is the number of cognitive user. Similarly, W_e is the noise power introduced by the eavesdropper receivers and I_e ($I_e = \sum_{i=1}^{n} P_e / d_{e,i}^{\alpha}$) is the interference power of the eavesdroppers from the cognitive users. Considering the main link and the eavesdropper, secrecy capacity satisfies $C_s = \max\{C_p - C_e, 0\}$.

3.2 Summary of PHY layer security

From above overviews, the PHY layer security has been given a brief introduction in an information-theoretic point of view, which has attracted considerable attention recently. The basic idea is to exploit the physical characteristics of the wireless channel in order to transmit messages securely. In the conventional wireless network, the wire-tapper that eavesdrop information from the main channel is a kind of passive threat to the system. However, Physical layer security approaches for wireless communications can prevent eavesdropping without upper layer data encryption, which can reduce the computational and communication overheads while encryption brings additional system complexity for the secret key distribution and management. Moreover, wiretaps issue has been expanded to cognitive radio network. By exploring the physical layer security, it can effectively improve the capacity and reliability of CRNs without the higher layer security arrangement, such as encryption.

IV. Discusion Future Work in CRNs

In this paper, we have investigated the security issues in cognitive radio network from active attack and passive attack respectively. However, the security considerations in CRNs setting are still in their infancy phase and require a more thorough analysis by the research community. In this section, we will briefly discuss the direction and expectations of the future pursuit about security issue in CRNs.

4.1 From the security capacity perspective

It is known that capacity is an optimal indicator to measure the quality of a network, and security capacity is an indicator to measure the network security effectiveness. In section 3, the secrecy capacity has been derived from the information-theoretic security with the threat of eavesdropping. Are there relationships between the capacity and other parameters, such as outage probability and interference probability of success that from malicious interference and attack, and so on? Hence, we give a prospect that there is a unified security capacity expression which not only include eavesdropping channel causing the information leakage, but also the attacker forcibly occupy channel causing the interruption of information transmission. This means that there should be an evolution definition of secrecy capacity as security capacity that contains the secrecy capacity caused by passive attacks and outage capacity caused by active attacks.

Assume a simple hypothetical model where there is a communication link between two cognitive users, transmitter (Alice) and intended receiver (Bob). However, there are two

evildoers access to this link distinguished from Wyner model [68], which one is eavesdropper (Eve) a passive attacker and the other is intruder (Tudor) an active attacker, as shown in Fig. 6. It will give us some enlightenment to derive the united security capacity expression from the two basic types of attack.

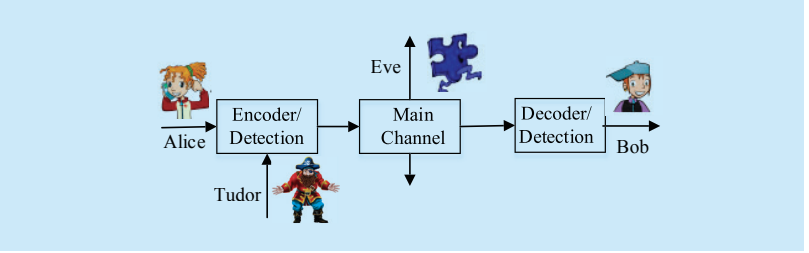

Fig.6 *The novel security capacity model*

4.2 From the countermeasures perspective

In the overall security defense, there are three phases of countermeasures to address the security issues in CRNs.

1) *The prophase provides an essential security blanket*

The prophase contains encryption [87] and authentication [88] for defensing the wiretap, which are the important components in conventional security scheme that occur in the upper layer of the network protocol stack. Public key encryption based primary user identification is proposed in [89] to prevent secondary users masquerading as primary users. Legitimate primary users are required to transmit an encrypted value (signature) along with their transmissions which is generated using a private key. This signature is used for validating the primary user. However, this method can only be used with digital modulations. Furthermore, secondary users should have the capability to synchronize and demodulate primary users' signal.

Furthermore, the encryption can be difficult to manage while in a peer-to-peer network such as an ad hoc network, or cognitive radio network, for key management becomes more and more complicated as the number of nodes increases. The idea of exploiting the imperfections of the physical layer as a first layer of defense has recently attracted much interest and is now colloquially known as physical-layer security [90]. In PHY layer, the secrecy codes may provide security enhancements or standalone security solutions. PHY layer security approaches for wireless communications can prevent eavesdropping without upper layer data encryption.

However, PHY layer security is hampered by the wireless channel conditions, namely, absent feedback, and it is typically feasible only when the source-destination channel is better than the source-eaves-dropper channel. Areas that warrant further research include performance degradation in the presence of imperfect channel estimates, and optimization based on partial channel knowledge only, e.g., only statistical information about the eavesdropper's channels is available, or each relay only knows its own channel. In those cases, other metrics such as ergodic secrecy rate, or outage probability could be employed. Also, design under alternative network scenarios would be of interest, such as scenarios where there is only one relay equipped with multiple antennas, or there is a single eavesdropper equipped with multiple antennas. Further study is needed for the case in which the number of relays is no greater than the number of eavesdroppers [78].

Moreover, extensions to two-way relay channels and multi-hop networks are also of interest. And it is also important to study the impact of these secrecy-based physical layer transmission schemes on modern communication systems, such as cognitive radio and ad hoc networks. For example, in cognitive radio applications, Artificial Noise transmissions by secondary users should be carefully designed so that they do not cause excessive interference at primary users [79]. The multi-antenna systems, channel precoding and power allocation techniques attract researchers' attention [91], which can enhance secrecy by significantly degrading the ability of an unintended receiver to obtain useful waveforms due to differences in channel characteristics.

2) *The metaphase provides an active mid-course defense*

The metaphase is attack detection that most of the studies in security of CRN focus on, and the existing achievement discussing detailed approaches for the detection and mitigation of specific attacks have been summarized in section 2.2. A number of threats specifically pertain to cognitive communications, most notably to secure the spectrum sensing process against exogenous and insider malicious nodes.

Firstly, for PUEA, there are many detection techniques that have been investigated and most of them utilize energy detection technique for spectrum sensing. Although energy detection is the most widely used spectrum sensing technique, it cannot provide reliable results because of the uncertainty of the noise level in very dynamic environments. Thus, new security techniques based on other spectrum sensing methods like matched filter detection, and cyclostationary feature detection mixed together should be investigated.

Secondly, most techniques for the detection of SSDF attacks consider a centralized entity (base station or fusion center that collects observations and decides upon the absence/presence of incumbent signals. The advantage of these techniques is cooperative spectrum sensing where a number of users exchange messages with the FC. It is easy for cognitive radio network to detect and discard the malicious reports by using this centralized scheme. However, a major disadvantage of this scheme is that the FC can become a single point of failure if successfully attacked by malicious users. Moreover, an attacker can cause severe DoS attacks, including congestion, cheating and jamming to the FC, which makes the whole CRN completely inoperable.

Furthermore, unintentionally misbehaving attack, such as malfunctions or random failures (e.g. electricity black-out) will also disrupt the CRNs operation completely, which is a potential research direction. The far reaching effect of isolated attacks against CRNs, due to the learning-based interaction cognitive nodes with their wireless network environment, is another key issue to be more vigorously investigated.

3) *The anaphase provides a terminal intercept sanction*

The anaphase is how to dispose the attacks. Numerous researches of security issues have mainly focused on attacking detection based on source localization, attack signature, detection probability and other techniques in CRNs. However, few of them take the penalty of attackers into consideration and neglect how to implement effective punitive measures against attackers. A likely instance is that we cannot punish an offender, even though the person transgresses moral or civil law. The only thing we can do is offering the proof to legal operation department. Therefore, how to implement effective management to attack users will be one of the research directions. To address this issue, Security Management based on Trust Determination (SMTD) [23] is proposed for solving this issue in CRNs, which is based on reputation of nodes and punishment for misbehaving users under centralized control of FC. Moreover, reference [91] also presents the state of the art of Identity Management systems for security issues to realize the effective management of attackers, and points out that future communication intends to be more secure.

V. Conclusion

In this article, we have analyzed the security issues in cognitive radio networks and investigated the most important contributions on security threats and the current state of the art techniques. Firstly, we spot the security issues and provided a classifications of attacks in the CRNs. Secondly, we survey the existing countermeasures for defensing against the active attacks. Thirdly, we present the PHY layer security in the view-point of passive attacks. Finally, we further discuss the direction and expectations of the future pursuit about security issue in cognitive radio networks. It is our hope that this tutorial will provide a bridge for

researchers in many areas towards establishing complete security solutions that successfully integrate security system in cognitive radio networks.

Acknowledgements

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported in part by the National Natural Science Foundation of China (61227801, 61121001, 61201152, and 61421061), the Program for New Century Excellent Talents in University (NCET-01-0259) and the Fundamental Research Funds for the Central Universities (2013RC0106).

References

[1] Spectrum Efficiency Working Group, Spectrum policy task force report, Federal Communications Commission. http://www.fcc.gov/sptf/files/SEWGFinalReport_1.pdf. 2002

[2] P Zhang, "In the development of wireless cognitive science," Chin. Sci. Bull. 57, pp. 3661-3661. 2012

[3] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," IEEE Personal Commun., vol. 6, pp. 13-18, 1999.

[4] IEEE 802.22 Working Group, "IEEE P802.22/D1.0 draft standard for wireless regional area networks part 22: Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands," Apr. 2008.

[5] Y. Liang, H.V. Poor and S. Shamai (Shitz). Foundations and Trends in Communications and Information Theory. Information Theoretic Security NOW, pp. 355-580. 2008

[6] Fragkiadakis, A.G., Tragos, E.Z., Askoxylakis, I.G., "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks, " IEEE Communications Surveys and Tutorials 15, pp. 428-445. 2013

[7] Sumathi, A.C.; Vidhyapriya, R., "Security in cognitive radio networks - a survey,", 2012 12th International Conference on Intelligent Systems Design and Applications (ISDA), pp.114-118, Nov. 2012

[8] Yucek, T., Arslan, H., "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Communications Surveys & Tutorials, vol.11, no.1, pp.116-130, First Quarter 2009

[9] Yucek T, Arslan H. "Spectrum characterization for opportunistic cognitive radio systems, " In: Proceedings of Military Communication Conference, 2006, Washington DC: IEEE, pp. 1-6. 2006

[10] Quan Z, Shellhammer S J, Zhang W, et al., "Spectrum sensing by cognitive radios at very low SNR, " In: Proceedings of Global Communications Conference, 2009, Beijing, Washington DC: IEEE, pp. 1-6. 2009

[11] Tang H. "Some physical layer issues of wideband cognitive radio systems, " In: Proceedings of International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005, Baltimore, Maryland, Washington DC: IEEE, pp. 151-159. 2005

[12] Weidling F, Datla D, Petty V, et al., "A framework for RF spectrum measurements and analysis," In: Proceedings of International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005, Baltimore, Maryland, Washington DC: IEEE, pp. 573-576. 2005

[13] Lehtomaki L, Vartiainen J, Juntti M, et al., "Spectrum sensing with forward methods, " In: Proceedings of Military Communications Conference, 2006, Washington DC: IEEE, pp. 1-7. 2006

[14] Gardner U W. "Exploitation of spectral redundancy in cyclostationary signals, " IEEE Signal Process Mag, 8: pp. 14-36. 1991

[15] Muraoka K, Ariyoshi M, Fujii T. "A novel spectrum-sensing method based on maximum cyclic autocorrelation selection for cognitive radio system," In: Proceedings of 3rd Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2008, Dublin, Washington DC: IEEE, pp. 1-7. 2008

[16] Du K L, Wai H M. "Affordable Cyclo-stationarity-Based Spectrum Sensing for Cognitive Radio with Smart Antennas," IEEE Trans Veh Technol, 59: pp. 1877-1887. 2010

[17] Proakis J G. Digital Communications. 4th ed. McGraw-Hill, 2001

[18] Tandra R, Sahai A. Fundamental limits on detection in low SNR under noise uncertainty. In: Proceedings of International Conference on Wireless Networks, Communication and Mobile Computing, 2005, Maui, HI, Washington DC: IEEE, pp. 464-469. 2005

[19] Tandra R, Sahai A. SNR walls for signal detection. IEEE J Sel Top Sign Proces, pp. 4-17. 2008

[20] Cabric D, Mishra S, Brodersen R. Implementation issues in spectrum sensing for cognitive radios. In: Proceedings of Asilomar Conference on Signals, System, Computation, 2004, Washington DC: IEEE, pp. 772-776. 2004

[21] Cabric D, Tkachenko A, Brodersen R. Spectrum sensing measurements of pilot, energy, and collaborative detection. In: Proceedings of Military Communications Conference, 2006, Washington DC: IEEE, pp. 1-7. 2006

[22] Zesheng Chen, Cooklev, T., Chao Chen, Pomalaza-Raez, C., "Modeling primary user emulation

attacks and defenses in cognitive radio networks," Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International, pp.208-215, 2009

[23] Li J, Feng Z, Wei Z, Feng Z, Zhang P. "Security management based on trust determination in cognitive radio networks", EURASIP Journal on Advances in Signal. http://asp.eurasipjournals.com/content/2014/1/48. 7 Apr. 2014.

[24] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE J. Sel. Areas Commun. , vol. 26, pp. 25-37, 2008.

[25] Z. Jin and K. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in Proc. ICC, 2009, pp. 1-5. 2009

[26] Z. Jin, S. Anand, and K. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," in Proc. ACM SigMobile Computing and Communication Review, pp. 74-85. 2009

[27] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in Proc. of IPCCC, 2009, pp. 208-215. 2009

[28] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in Proc. 2010 IEEE Symposium on Security and Privacy, pp. 286-301. 2010

[29] Anand, S.; Jin, Z.; Subbalakshmi, K. P., "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on, pp.1,6, 14-17 Oct. 2008

[30] Zhiyao Ma; Wei Chen; Letaief, K.B.; Zhigang Cao, "A Semi Range-Based Iterative Localization Algorithm for Cognitive Radio Networks," IEEE Transactions on Vehicular Technology , vol.59, no.2, pp.704-717, Feb. 2010

[31] T. Aysal, S. Kandeepan, and R. Piesewicz, "Cooperative Spectrum Sensing with Noisy Hard Decision Transmissions," in Proc. ICC, 2009, pp. 1-5. 2009

[32] Y. Chen, "Collaborative spectrum sensing in the presence of secondary user interferences for lognormal shadowing," Wireless Communications and Mobile Computing, Volume 12, Issue 5, pages 463-472, 10 April, 2012

[33] J. Meng, W. Yin, H. Li, E. Houssain, and Z. Han, "Collaborative spectrum sensing from sparse observations using matrix completion for cognitive radio networks," in Proc. ICASSP, 2010, pp. 3114-3117. 2010

[34] Bin Shen; Kyungsup Kwak; Zhiquan Bai, "Optimal Linear Soft Fusion Schemes for Cooperative Sensing in Cognitive Radio Networks," Global Telecommunications Conference, 2009. IEEE, pp.1-6. 2009

[35] Zarrin, S.; Teng Joon Lim, "Cooperative Quickest Spectrum Sensing in Cognitive Radios with Unknown Parameters," Global Telecommunications Conference, 2009. IEEE, pp.1-6. 2009

[36] Z. Tian, E. Blasch, W. Li, G. Chen, and X. Li, "Performance evaluation of distributed compressed wideband sensing for cognitive radio networks," in Proc. ISIF, 2008, pp. 1-8. 2008

[37] Husheng Li; Ju Bin Song; Chien-fei Chen; Lifeng Lai; Qiu, R.C., "Behavior Propagation in Cognitive Radio Networks: A Social Network Approach," Wireless Communications, IEEE Transactions on , vol.13, no.2, pp.646-657, February 2014

[38] Husheng Li; Chien-fei Chen; Lifeng Lai, "Propagation of Spectrum Preference in Cognitive Radio Networks: A Social Network Approach," Communications (ICC), 2011 IEEE International Conference on , vol., no., pp.1-5, June 2011

[39] Z. Jin, S. Anand, and K. P. Subbalakshmi, "NEAT: A neighbor Assisted Spectrum decision protocol for resilience against Primary User emulation attacks," Technical Report, Dec. 2009.

[40] Jin, Z.; Anand, S.; Subbalakshmi, K.P., "Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE , pp.1-5, Dec. 2010

[41] Kaligineedi, P.; Khabbazian, M.; Bhargava, V.K., "Malicious User Detection in a Cognitive Radio Cooperative Sensing System," Wireless Communications, IEEE Transactions on , vol.9, no.8, pp.2488-2497, August 2010

[42] Mishra, A.; Nadkarni, K.; Patcha, A., "Intrusion detection in wireless ad hoc networks," Wireless Communications, IEEE, vol.11, no.1, pp.48-60, Feb 2004

[43] Butun, I.; Morgera, S.D.; Sankar, R., "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," Communications Surveys & Tutorials, IEEE , vol.16, no.1, pp.266-282, First Quarter 2014

[44] Fadlullah, Z.M.; Nishiyama, H.; Kato, N.; Fouda, M.M., "Intrusion detection system (IDS) for combating attacks against cognitive radio networks," Network, IEEE , vol.27, no.3, pp51-56. May-June 2013

[45] Caidan Zhao; Wumei Wang; Lianfen Huang; Yan Yao, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio," Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on, pp.1,5, 24-26 Sept. 2009

[46] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Countering byzantine attacks in cognitive radio networks," in Proc. ICASSP, 2010, pp. 3098-3101. 2010

[47] R. Chen, J. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in Proc. Milcom, 2008, pp. 1876-1884. 2008
[48] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in Proc. CISS, 2009, pp. 130-134. 2009
[49] F. Zhu and S. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," Journal of Communications and Networks, vol. 11, pp. 122-133, 2009.
[50] F. Yu, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in Proc. Milcom, 2009, pp. 1-7. 2009
[51] N. Nhan and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," IEEE Commun. Lett., vol. 13, pp. 492-494, 2009.
[52] G. Shafer, A Mathematical Theory of Evidence. Princeton University Press, 1976.
[53] A. Min, K. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in Proc. ICNP, pp. 294-303. 2009
[54] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in DySPAN, 2010, pp. 1-12. 2010
[55] Ding, G., Wu, Q., Yao, Y., Wang, J., Chen, Y.: Kernel-Based learning for statistical signal processing in cognitive radio networks. IEEE SIGNAL PROCESSING MAGAZINE 30, pp.126-136. 2013
[56] Ding, G., Wang, J., Wu, Q., Song, F., Chen, Y.: Spectrum sensing in Opportunity-Heterogeneous Cognitive Sensor Networks: How to Cooperate?. IEEE SENSORS JOURNAL 13, pp.4247-4255. 2013
[57] Xiaofan He; Huaiyu Dai; Peng Ning, "A Byzantine Attack Defender in Cognitive Radio Networks: The Conditional Frequency Check," Wireless Communications, IEEE Transactions on , vol.12, no.5, pp.2512-2523, May 2013
[58] J. Fitton, "Security considerations for software defined radios," in Proc. SDR '02 Technical Conference and Product Exposition, pp. 1-7. 2002
[59] C. Li, A. Raghunathan, and N. Jha, "An architecture for secure software defined radio," in Proc. Date '09, pp. 448-453. 2009
[60] Shucai Xiao; Jung-Min Park; Yanzhu Ye, "Tamper Resistance for Software Defined Radio Software," Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International , pp.383-391, July 2009
[61] A. Brawerman, D. Blough, and B. Bing, "Securing the download of radio configuration files for software defined radio devices," in MobiWac, 2004, pp. 98-105. 2004
[62] H. Uchikawa, K. Umebayashi, and R. Kohno, "Secure download system based on software defined radio composed of fpgas," in PIMRC, 2002, pp. 437-441. 2002
[63] J. Campbell, W. Campbell, D. Jones, S. Lewandowski, D. Reynolds, and C. Weinstein, "Biometrically enhanced software-defined radios," in Proc. Software Defined Radio Technical Conference, pp. 1-6. 2003
[64] Poor, H.V., "Information and inference in the wireless physical layer," Wireless Communications, IEEE , vol.19, no.1, pp.40-47, February 2012
[65] Yulong Zou; Xianbin Wang; Weiming Shen, "Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks," IEEE Transactions on Communications, vol.61, no.12, pp.5103-5113, December 2013
[66] Zhihui Shu; Yi Qian; Song Ci, "On physical layer security for cognitive radio networks," Network, IEEE , vol.27, no.3, pp.28-33. 2013
[67] C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, pp. 656-715, 1949.
[68] A. D. Wyner, "The wiretap channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.
[69] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, pp. 339-348, 1978.
[70] S. K. Leung-Yan-Cheong and Martin E. Hellman. "The Gaussian Wire-tap Channel," IEEE Trans. Inform. Theory, 24(4):451-456, July 1978.
[71] Imre Csisz´ar and Prakash Narayan. "Secrecy Capacities for Multiple Terminals," IEEE Trans. Inform. Theory, 50(12):3047-3061, December 2004.
[72] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in proc. IEEE ISIT 2006, pp. 356-360, July 2006.
[73] Gopala, Praveen Kumar; Lifeng Lai; El-Gamal, H., "On the Secrecy Capacity of Fading Channels," Information Theory, IEEE Transactions on , vol.54, no.10, pp.4687-4698, Oct. 2008
[74] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel with collective secrecy constraints," IEEE ISIT 2006, pp. 1164-1168, July 2006.
[75] Y. Liang, H. V. Poor and S. Shamai, "Secure communication over fading channels," IEEE Transactions on Information Theory, VOL. 54, NO. 6, Page(s): 2470-2492. June 2008
[76] Zhu Han; Marina, N.; Debbah, M.; Hjorungnes, A., "Improved Wireless Secrecy Rate Using Distributed Auction Theory," Mobile Ad-hoc and Sensor Networks, 2009. MSN '09. 5th International Conference on , pp.442-447, Dec. 2009
[77] Lifeng Lai; El Gamal, H., "The Relay–Eavesdropper Channel: Cooperation for Secrecy," Information Theory, IEEE Transactions on , vol.54, no.9, pp.4005-4019, Sept. 2008

[78] Lun Dong; Zhu Han; Petropulu, AP.; Poor, H.V., "Improving Wireless Physical Layer Security via Cooperating Relays," Signal Processing, IEEE Transactions on , vol.58, no.3, pp.1875-1888, March 2010
[79] Hong, Y.-W.P.; Pang-Chang Lan; Kuo, C.-C.J., "Enhancing Physical-Layer Secrecy in Multiantenna Wireless Systems: An Overview of Signal Processing Approaches," Signal Processing Magazine, IEEE , vol.30, no.5, pp.29-40, Sept. 2013
[80] Anand, S.; Chandramouli, R., "On the Secrecy Capacity of Fading Cognitive Wireless Networks," Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on , pp.1-5, May 2008
[81] M. Vu, N. Devroye and V. Tarokh, "The Primary exclusive region in cognitive networks," Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE , pp.1014-1019, Jan. 2008
[82] Vu, M.; Tarokh, Vahid, "Scaling laws of single-hop cognitive networks," IEEE Transactions on Wireless Communications, vol.8, no.8, pp.4089-4097, August 2009
[83] Peng Jia; Vu, Mai; Le-Ngoc, Tho, "Capacity Impact of Location-Aware Cognitive Sensing," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pp.1-6, 2009
[84] Mohammad G. Khoshkholgh, Keivan Navaie, and Halim Yanikomeroglu, "Access Strategies for Spectrum Sharing in Fading Environment: Overlay, Underlay, and Mixed, " IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 12, DECEMBER 2010
[85] Zhihui Shu, Yaoqing Yang, Yi Qian, Hu, R.Q., "Impact of Interference on Secrecy Capacity in a Cognitive Radio Network," Global Telecommunications Conference, 2011. IEEE, pp.1-6. 2011
[86] A. Goldsmith, Wireless Communications, Cambridge University Press, 2005.
[87] Kaliski, B., "A survey of encryption standards," Micro, IEEE , vol.13, no.6, pp.74-81, Dec. 1993
[88] Kilinc, H.; Yanik, T., "A Survey of SIP Authentication and Key Agreement Schemes," Communications Surveys & Tutorials, IEEE , pp.1-19, 2013
[89] C. N. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in First IEEE Workshop on Cognitive Radio Networks, Las Vegas, Nevada, USA, pp. 1037-1041. 2007
[90] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[91] Harrison, W.K., Almeida, J., Bloch, M.R., McLaughlin, S.W., Barros, J., "Coding for Secrecy: An Overview of Error-Control Coding Techniques for Physical-Layer Security," Signal Processing Magazine, IEEE , vol.30, no.5, pp.41-50, Sept. 2013
[92] Jenny Torres, Michele Nogueira, and Guy Pujolle. "A Survey on Identity Management for the Future Network," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

Biographies

***LI Jianwu*,** is currently a Ph.D. candidate at Beijing University of Post and Telecommunications, Beijing, China. His research interests include spectrum detection on cognitive wireless networks, wireless networks security, security mechanisms, and the key techniques on integration of heterogeneous networks. Recently, he has participated in some projects, such as 973project, the NSFC projects and National Defense special projects. He is also a reviewer of KSII transactions on internet and information systems. Email: jianwu.lee@gmail.com

FENG Zebing, received his B.S. degree from Nanjing University of Science and Technology (NJUST) in 2011. He is currently studying towards the Ph.D. degree in Communication and Information Systems at the Wireless Technology Innovation (WTI) Institute of Beijing University of Posts and Telecommunications (BUPT). His research interests include the convergence of heterogeneous wireless networks, dynamic spectrum management and interference analysis, cognitive radio technology, and data mining. Email: happyfzb@gmail.com

FENG Zhiyong, received her M.S. and Ph.D. degrees from Beijing University of Posts and Telecommunications (BUPT), China. She is a professor at Beijing University of Posts and Telecommunications (BUPT), and is currently leading the Ubiquitous Network Lab in the Wireless Technology Innovation (WTI) Institute. She is a member of IEEE and active in standards development such as ITU-R WP5A/WP5D, IEEE 1900, ETSI and CCSA. Her main research interests include the convergence of heterogeneous wireless networks, dynamic spectrum management, joint radio resource management, cognitive wireless networks, cross-layer design, spectrum sensing, and self-x functions. Email: fengzy@bupt.edu.cn

***ZHANG Ping*,** received his Ph.D. degree in electrical from Beijing University of Posts and Telecommunications (BUPT), China in 1990. He is a Professor at the School of Information and Communication Engineering of BUPT. He is an Executive Associate Editor-in-Chief on information sciences of Chinese Science Bulletin, Reviewer and TCP Member of many magazines, journals and conferences. He is a Member of next-generation broadband wireless communication network in National Science and Technology Major Project, a Member of the 5th Advisory

Committee of National Natural Science Foundation of China, the Chief Scientist of "973" National Basic Research Program of China, a Member of the 11th Beijing Municipal Committee of Chinese People's Political Consultative Conference, and the owner of the Special Government Allowance of State Council of China. He received the Second Award for National Science and Technology Prize twice, the Second Award for National Science and Technology Invention Prize once, the Provincial Science and Technology Awards many times, and the Title of Outstanding Science and Technological Workers in 2010. His research interests include broadband wireless communication, new technologies on cognitive wireless networks, TD-LTE, MIMO, OFDM etc. Email: pzhang@bupt.edu.cn