On Physical Layer Security for Cognitive Radio Networks

Zhihui Shu, Yi Qian, and Song Ci, University of Nebraska-Lincoln

Abstract

In this article we explore the security issues on physical layer for cognitive radio networks. First we give an overview on several existing security attacks to the physical layer in cognitive radio networks. We then discuss the related countermeasures on how to defend against these attacks. We further investigate one of the most important physical layer security parameters, the secrecy capacity of a cognitive radio network, and study the outage probability of secrecy capacity of a primary user from a theoretical point of view. Furthermore, we present performance results for secrecy capacity and outage probability between a node and its neighbors. Our work summarizes the current advances of the physical layer security and brings insights on physical layer security analysis in cognitive radio networks.

Cognitive radio is a technology that can solve the wireless spectrum under-utilization problem by allowing secondary users to opportunistically access the licensed channels without causing interference to the communications of the primary users. Cognitive radio can change its transmitter parameters based on interaction with the environment in which it operates [1]. There are two main characteristics of cognitive radios. The first is cognitive capability, which refers to the ability of the radio technology to sense information from its radio environment. Through this capability, the spectrum resources that are not used by primary users can be detected. Consequently, the best spectrum allocation schemes and transmission parameters can be selected. The second is reconfigurability, which enables a user to change the transmitting channel quickly and adaptively according to the radio environment.

In a cognitive radio network there are mainly two schemes for secondary users to share the spectrum resources. In one scheme the secondary users reuse the spectrum that is not used by the primary users. The other scheme, called spectrum sharing, allows the secondary users to transmit concurrently with the primary users as long as they do not harm the transmission of the primary users. While cognitive radio is an efficient technique to relieve the pressure of wireless spectrum scarcity, at the same time the characteristics of cognitive radios have introduced entirely new types of security threats and challenges in networks. Since the primary users and the secondary users coexist in the same network, both of them need to be protected, and they are more vulnerable to security attacks compared to the traditional wireless networks without using cognitive radios. Therefore, providing strong security protections is one of the most important requirements for cognitive radio networks.

In general, wireless networks are deployed in homes, businesses, production plants, and other private or public environments where security of communications is important. Many publications have addressed practical attacks on the availability of IEEE 802.11 networks on both the physical layer (PHY) and the medium access control (MAC) layer. One of the traditional attacks at the PHY layer is jamming of the radio band. On the MAC layer, more sophisticated attacks could be implemented to attack the MAC protocols. The attacks could be grouped into three categories [2]:

- RF jamming attacks.
- MAC layer attacks.
- Implementation-specific attacks (driver/firmware).

Another way to investigate the security of wireless networks is from the information theoretic perspective.

In physical layer security for wireless networks, the secrecy rate is defined as the rate at which information can be transmitted secretly from a source to its intended destination. The maximum achievable secrecy rate is named the secrecy capacity. For a Gaussian channel, the secrecy capacity is defined as the difference of the Shannon capacity of the channel between the source and the destination and the Shannon capacity of the channel between the source and an eavesdropper [3]. Besides secrecy capacity, there are also some other parameters that depict the security of wireless networks. One is the leakage probability, which is the probability that the eavesdropper decodes its received codeword with an error probability less than its target bit error rate. Another is the security gap [4], which is the ratio of two signal-to-noise ratios (SNRs), the SNR at which a very low-target bit error rate (BER) is achieved at the intended receiver, and that at which a high BER is achieved at the eavesdropper. The smaller the security gap, the more likely that the transmitter can transmit over a time-varying wireless channel successfully. In wireless networks, physical layer security can provide the theoretical analysis about how much information a user can transmit safely with the existence of eavesdroppers. However, the analysis in cognitive radio networks is more difficult since we need to consider both the primary users and the secondary users.

Although security in classic wireless networks has been studied for many years, security in the physical layer of cognitive radio networks has not been well investigated until recently. In [5] and [6] the authors studied two major classes of attacks on the physical layer in cognitive radio networks:

0890-8044/13/$25.00 © 2013 IEEE

Attacks	Countermeasures	Characteristics
PUE [5]	LocDef [7] based on localization of the primary user	Verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics
OFA [8]	Define threshold values whenever the radio parameters need to be updated [5]	A good intrusion detection system can be used
LA [8]	Effective and long-term learning [8]	The learning results must always be reevaluated over time
SSDF [6]	Powerful schemes at data fusion center [9]	Sequential Probability Ratio Test or reputation-based schemes
Jamming [10]	Frequency hopping or spatial retreat [6, 11]	Frequency hopping is good for cognitive radios
Eavesdropping [12]	Power control or beamforming [12]	Theoretical results to provide some general bounds

Table 1. *The attacks and the countermeasures of physical layer security in cognitive radio networks.*

primary user emulation attack and objective function attack. There are also several other types of attacks and the corresponding countermeasures on the physical layer in cognitive radio networks. In this article we first systematically survey different types of attacks on the physical layer and their corresponding countermeasures in cognitive radio networks. Specifically, we summarize six major types of attacks: primary user emulation; objective function attack; learning attack; spectrum sensing data falsification; jamming attack; and eavesdropping. To emphasize the importance of physical layer security issues in cognitive radio networks, we present an analysis method of secrecy capacity in a cognitive radio network model, to characterize how much information a user can transmit safely with the existence of eavesdroppers in cognitive radio networks.

The characteristics of cognitive radio networks have brought new challenges to physical layer security issues. First, there are both primary users and secondary users in the network. The secondary users should have the ability to tell the difference between primary users and malicious nodes. Second, the accuracy of sensing information gathered by secondary users is important. However, malicious users may attack and interfere with the correct sensing information. Third, much fundamental theoretic analysis has not been done yet to reveal the physical layer security of cognitive radio networks with the existence of primary users, secondary users, and other malicious nodes.

In the rest of this article we first briefly overview the physical layer security issues in cognitive radio networks. We discuss several known security attacks existing in cognitive radio networks and survey the related countermeasures on how to defend against these attacks. Then we investigate one of the most important physical layer security parameters, the secrecy capacity of a cognitive radio network, by studying the probability density function of the secrecy capacity and obtaining the outage probability of secrecy capacity. At the end, we provide performance results and summarize the study of physical layer security in cognitive radio networks.

Current State-of-the-Art on PHY Security in Cognitive Radio Networks

In recent years there have been several major types of threats and attacks on the physical layer of cognitive radio networks, which we summarize in Table 1.

Primary User Emulation Attack

The first is the primary user emulation (PUE) attack [5]. A PUE attacker may masquerade as a primary user by transmitting special signals in the licensed band, thus preventing other secondary users from accessing that band. In PUE attacks, the attacker only transmits on the channels that are not used by primary users. Therefore, the secondary users regard the attackers as primary users and do not try to access the channels that are not used by primary users. As pointed out in [6], there are several types of PUE attacks. In a selfish PUE attack, an attacker tries to make use of the unused spectrum. When a selfish PUE attacker detects an unused spectrum band, it transmits signals that emulate the signal characteristics of a primary user and prevent the secondary users from using it. Thus, the attacker can make use of the vacant channels that are not used by primary users. However, for a malicious PUE attack, the malicious attacker just tries to prevent the transmission of the secondary users without using it. There exist some more complicated PUE attacks. Some attackers can even attack only when the primary user is off, which means that attackers can save energy.

To defend against this threat, a transmitter verification scheme called localization-based defense (LocDef) was proposed in [7], which verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. In a practical case of cognitive radio networks, the primary users can mainly be composed of TV signal transmitters (i.e. TV broadcast towers) and receivers. Their locations are typically determined. If a malicious user wants to emulate the primary user and its location is almost the same as the primary user, secondary users would not receive the signal of the malicious user since the transmit power of the malicious node is much smaller than a TV tower. If the secondary users receive a high power signal from the malicious user, it means that the malicious user must be very close to the secondary user. Thus, the secondary user can determine whether a transmitter is a primary user or malicious user just by estimating the location of the transmitter. The transmitter verification scheme includes three steps: verification of signal characteristics, measurement of received signal energy level, and localization of the signal source. The first two steps have been investigated thoroughly. For the third step, there are many techniques that can be used to estimate the location of the transmitter, such as Time of Arrival (TOA), Time Difference Of Arrival (TDOA), Angle of Arrival (AOA), and Received Signal Strength (RSS). Take RSS as an example: there is a strong correlation between the distance of a wireless link and RSS. Therefore, if multiple secondary users take RSS measurements from a transmitter, the transmitter location can be estimated using the relationship between distance and RSS. Thus, the key to counter against PUE attack is to determine whether the transmitter is a primary user or a malicious user.

Objective Function Attack

Another attack on cognitive radio networks is the objective function attack (OFA) [8]. This attack mainly targets the learning engine of cognitive radios. In cognitive radios, a cognitive engine has the ability to tune many parameters to maximize its objective function. These objective functions take as variables high transmission data rate, low power consumption, low delay, and high security level. Such parameters might include bandwidth, power, modulation type, coding methods, MAC protocol, routing schemes, and encryption mechanisms [6]. Among those variables of the objective function, high transmission rate and low delay are related to the channel, while low power consumption and high security level are directly determined by the inputs of the users. So for an objective function attack, whenever the user wants to raise the security level, the malicious nodes may use some ways to increase the delay of the user. Thus, the user may connect high delay with high security level and not want to use high security level at all. Thus, it will become more susceptible to security attacks. It is necessary to remark that the OFA performance is related to which optimization method is used in the cognitive radio network [8]. Some cognitive radios perform optimization instantly after getting the input of the environment. On the other hand, other cognitive radios observe the environment just once, then search for an optimized result, and the decision will not be changed by the input of the environment. In this case, the type of cognitive radio is not affected by OFAs. However, cognitive radio devices generally have high sensing ability and perform optimization frequently. Therefore, a cognitive radio network is susceptible to OFA attacks.

In order to combat an objective function attack, a simple suggestion has been made in [5]. It is to define threshold values whenever the radio parameters need to be updated. If the detected parameters do not meet the predefined thresholds, the secondary user will not collect that information. Moreover, a good intrusion detection system can be used to strengthen the countermeasure. However, using an intrusion detection system is a general countermeasure that may not perform well in defending against objective function attacks [6].

Learning Attack

In a learning attack (LA) [8] the adversary provides false sensory input for the learning radio in cognitive radios. If a learning radio learns some wrong ideas about the transmission schemes, it will be used all the way until it can learn the correct ideas. Generally, a learning attack is combined with other types of attacks. For example, an attacker can conduct a PUE attack or an OFA attack whenever a cognitive radio tries to use the best transmission scheme. Thus, the learning radio might decide that the best transmission scheme will not be optimal and it will take sub-optimal transmission schemes as the optimal transmission schemes, which leads to lower performance.

Several methods have been proposed to combat learning attacks [8]. First, the learning results must always be reevaluated over time. For example, the activities of the primary users in a cognitive radio network should be constantly recomputed so that the previously learned statistical process of activities of the primary users that may be incorrect will be abandoned. Second, there should be a truly controlled environment during the learning phases, which means no malicious signals are present during the learning phase. Third, if the learned action breaks some basic theoretic results, then this action should not be used. Fourth, cognitive radios can make use of group learning instead of individual learning. Several secondary users can form a group to learn the environment, and thus the attacker cannot conduct a learning attack so easily.

Spectrum Sensing Data Falsification

Spectrum Sensing Data Falsification (SSDF) is discussed in [6]. Also known as the Byzantine Attack, it is a popular attack in cognitive radio networks. An attacker sends false local spectrum sensing results to its neighbors or to the fusion center, causing the receiver to receive the wrong sensing information and make a wrong spectrum access decision. This attack can target the fusion center or just one secondary user. If it attacks the secondary user and sends wrong sensing information to just one secondary user, the secondary user may not have the ability to tell the real sensing information from the wrong sensing information and then make wrong decisions. While the attack targets the fusion center, the fusion center can collect sensing information from many other users, either legitimate secondary users or malicious users. If most of the sensing information is from legitimate users, the fusion center will have a high probability to make a right decision to determine which information would be real.

A two-level defense is required to counter SSDF attacks effectively [9]. At the first level, the data fusion center needs to authenticate all local spectrum sensing results since there might be malicious users who will eavesdrop the spectrum sensing results and then launch replay attacks or inject false data. The second level of defense is to implement an effective data fusion scheme that can determine which sensing information is real. There are several ways to improve existing data fusion schemes to counter SSDF attacks. One way is the Sequential Probability Ratio Test (SPRT). SPRT can support a large number of spectrum sensing results and combine them together. In this way, SPRT can have a higher probability to guarantee the spectrum sensing correctness. Another way is to use a reputation-based scheme in the Distributed Spectrum Sensing (DSS) process. This scheme can make a long time record of the sensing results and rate the users according to the correctness of their sensing results. Those who are always right can get a high reputation, and their results would be adopted. However, the malicious nodes would be low rated and would not be believed.

Jamming Attack

Another attack on cognitive radio networks is the jamming attack, which can be classified as a single-channel jamming attack or a multi-channel jamming attack [10]. In a single-channel jamming attack the malicious node continuously transmits high-power signals on one channel. Therefore, all transmissions on this channel will be jammed. However, this type of jamming is not so effective, since the malicious node should transmit continuously, which consumes much energy. Moreover, the high power interfering signal can be easily detected. Another more effective way of jamming is to jam multiple channels simultaneously. The traditional way is to transmit interfering signals on all the channels at the same time. However, this still consumes too much energy, especially when the number of channels is large. An improved way is to use cognitive radio technology so that the attacker can switch from one channel to another according to the activities of the primary users. Since cognitive radios can significantly reduce channel switching delay, attackers can jam the channel more effectively in this way.

To counter jamming attacks, secondary users first need to detect that a jamming attack really exists. One way to detect a jamming attack is to collect enough data of the noise in the network and build a statistical model [11]. Thus, when an attacker tries to jam the secondary user and transmits large power interference, the secondary user can have the ability to differentiate the interference of an attacker from normal noise. The second step to counter a jamming attack is to defend against it, mainly

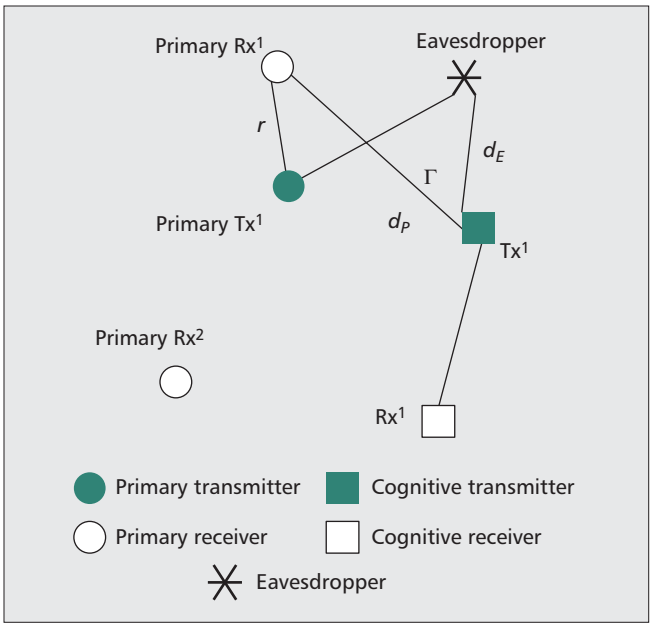

Figure 1. *A cognitive radio network model for secrecy capacity analysis.*

in two ways [6]. One is to use frequency hopping. Whenever the secondary users find the jamming attack, they will use their high switching ability to switch to other channels that are not jammed. Another way is to do spatial retreat. The secondary users may escape from the location where jamming happens to where there is no jammer. Thus, the interfering signals transmitted by the jammer will not be received by the secondary users. The disadvantage of this method is that spatial retreat may make the secondary user lose communication with the users it is now communicating with.

Eavesdropping

The last security threat we survey here is eavesdropping, which means that a malicious node would listen to the transmission of the legitimate users. In [12] the authors considered a network model in which the secondary users use multiple input multiple output (MIMO) transmission, the primary users use a single antenna, and the eavesdroppers can use either multiple antennas or a single antenna. The authors studied the achievable rates of the MIMO secrecy rate between secondary users and formed a non-convex max-min problem to maximize secrecy capacity without interfering with the primary users. The maximum achievable secrecy rate can be obtained by optimizing the transmit covariance matrix in the case of Gaussian input. Algorithms were proposed to compute the maximum achievable secrecy rate for the case of single-antenna eavesdroppers, and bounds on the achievable secrecy rate were obtained for general cases with multi-antenna secrecy and eavesdropper receivers. Here we can see that the key idea behind [12] is using power control algorithms in order to increase the rate between the legitimate users while decreasing the rate to the eavesdroppers. Thus, secrecy rate can be improved.

A Cognitive Radio Network Model for Secrecy Capacity Analysis

In the rest of this article, we present an analysis method of secrecy capacity in a cognitive radio network model. We assume that eavesdroppers are randomly deployed and they are not colluding. Secrecy capacity is one of the most important physical layer security parameters for cognitive radio networks [12, 13]. As illustrated in Fig. 1, a set of primary users, secondary users and eavesdroppers coexist in a cognitive radio network, where they follow the mutually independent homogeneous Poisson process [14] with densities λ_P, λ_S and λ_E, respectively. From Fig. 1, node 1 is the primary transmitter, which transmits to other primary receivers in the network. The secondary users transmit on the same channel as the primary transmitter using a smaller power in order not to cause too much interference to primary users. The eavesdropper tries to listen to the information that the primary transmitter is transmitting. Since the distance of primary receiver 1 to the primary transmitter 1 is the closest, we define primary receiver 1 as the closest neighbor of primary transmitter 1 as its distance to the primary transmitter 1 is the shortest. Similarly, primary receiver 2 is defined as the second closest neighbor of primary transmitter 1 since its distance to the primary transmitter 1 is the second shortest, and so on.

Assuming that the entire network is a circular region of radius R, where we analyze the features of this network in a large network with R going to infinity. In a quasi-static wireless environment, the received power $P_{rx}(x_i, x_j)$ at the primary receiver x_j should increase as the increase of the transmit power P of the primary transmitter, and the amplitude $|h(\overrightarrow{x_i, x_j})|$ of the complex fading coefficient of the primary link $\overrightarrow{x_i x_j}$ between the primary transmitter and primary receiver. Moreover, the received power would decrease if the distance d_{ij} between primary transmitter x_i and primary receiver x_j increases. Moreover, the wireless propagation is related to the path loss exponent, which varies from 0.8 to 4 due to different communication environment [15]. We consider the case $\alpha > 2$ here in order to calculate the interference from the secondary users to the primary users and the eavesdroppers.

Assuming that W_P is the noise power introduced by the primary receivers and I_P is the interference power at the primary receiver from the secondary users. We now consider a special case that there is only path loss $h(x_i, x_j)$ in the wireless environment, and it is normalized to be one for all i not equal to j. The thermal noise powers at the primary users and eavesdroppers are assumed to be the same because these noise powers can be assumed to be independent from the location of a secondary user and they are both W. The received powers at the primary users and the eavesdroppers can all be calculated by the propagation laws of wireless transmission. Thus, the secrecy capacity can be simplified as [13]:

$$C_s(x_i, x_j) = \max\left\{ \begin{array}{l} \log_2\left(1 + \dfrac{P}{\left\|x_i - x_j\right\|^{\alpha}\left(W + I_P\right)}\right) \\ -\log_2\left(1 + \dfrac{P}{\left\|x_i - e^*\right\|^{\alpha}\left(W + I_E\right)}\right), 0 \end{array} \right\}. \quad (1)$$

We can first derive the probability density function of I_P and I_E. Then, the probability density function of the secrecy capacity $C_s(i, j)$ is

$$f_{C_s(i,j)}(c) = \begin{cases} f_{C_P(i,j)}(c) * f_{C_E}(-c), & c > 0, \\ Pr_{0,j} \cdot \delta(c), & c = 0, \\ 0, & c < 0. \end{cases} \quad (2)$$

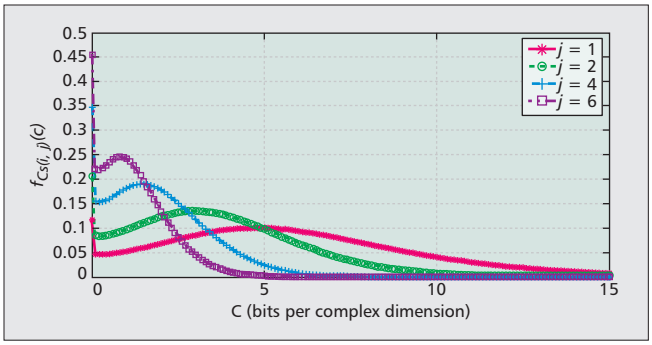

Figure 2. *Probability density function* $f_{C_s(i,j)}(c)$ *of the secrecy capacity* $C_s(i,j)(c)$ *for various* j.

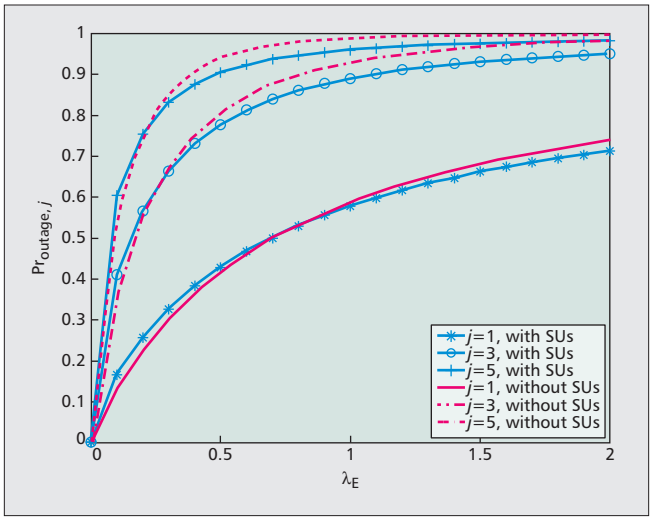

Figure 3. *Outage probability of secrecy capacity* $C_s(i,j)$ *for various values of* j ($\lambda = 1$, $\lambda_S = 0.1$ *(with secondary users (SUs)),* $R_s = 1$*).*

where i is the transmitter of a primary user, and j is the jth closest neighbor of the transmitter i, and $f_{C_P(i,j)}(c)$, $f_{C_E}(c)$, $\delta(c)$ and $Pr_{0,j}$ denote the probability density function of the primary user capacity, the probability density function of the eavesdropper capacity, the Dirac delta function, and the probability of zero secrecy capacity, respectively [13].

Secrecy Capacity Performance and Discussions

In this section, we show the performance results of our analysis above, and discuss the relationship between secrecy capacity, outage probability, and the densities of the primary users, the secondary users, and the eavesdroppers for some specific cognitive radio network scenarios. Here, the outage probability of secrecy capacity is defined as the probability that secrecy capacity is lower than a threshold R_s. For a certain threshold R_s, if the outage probability of secrecy capacity is high, it means that the communication link between legitimate users is not secure enough.

In the following, we use simulations to examine the performance results for secrecy capacity and outage probability between a node and its neighbors. In the performance results, the node densities and power parameters are set as the following. The density of primary users λ is 1, the densities of secondary users λ_S and eavesdroppers λ_E are both 0.1, the transmit power P of primary transmitter is 10 Watts, secondary transmitter P_s is 1 Watt, and noise power W is also 1 Watt. Moreover, in order to calculate the outage probability, the threshold rate R_s is set to be 1.

Figure 2 shows the relationship between probability density function $f_{C_S(i,j)}(c)$ and the secrecy capacity $C_s(i,j)$ between a node i and its jth closest neighbor. It can be seen that as the distance to the jth closest neighbor increases with j, it has a higher probability that the secrecy capacity has a smaller value. Figure 3 shows the relationship between secrecy outage probability and the eavesdropper density λ_E in different cases. It can be seen that the outage probability of secrecy capacity increases as j increases. Moreover, the outage probability of secrecy capacity will also increase as the density of eavesdroppers λ_E increases. When $j = 1$, we can see that two curves have an intersection at about $\lambda_E = 0.7$. When λ_E is smaller than 0.7, the network with secondary users has a higher outage probability. However, when λ_E exceeds 0.7, the network without secondary users has a higher outage probability. This means that when the density of eavesdroppers increases, they have a higher probability that they are close to the secondary users. Thus, the interference powers at the eavesdroppers would become higher and the information leaked to the eavesdroppers will decrease. Then, there would be lower outage probability and higher secrecy capacity in this case. The tendency is similar for the case of other values of j. Figure 4 illustrates the relationship between secrecy outage probability and the secondary user density λ_S. Similar to the case with secondary users in Fig. 3, the outage probability of secrecy capacity increases as j and the density of secondary users λ_S increase. This means that when the density of the secondary users is larger, the secrecy capacity will decrease and the outage probability of secrecy capacity will be larger. This is because the secondary users will be closer to the primary user in this case, and the interference powers at the primary users will be larger.

The performance results have shown how the densities of primary users and eavesdroppers influence the secrecy capacity and outage probability between a node and its neighbors. Secrecy capacity gives us a good upper bound on how much secure information can be transmitted in cognitive radio networks, but it does not indicate how we can achieve this secrecy capacity. Many other mechanisms should be used to achieve it. Moreover, secrecy capacity of a cognitive radio network can theoretically show how securely the information is transmitted in the network. Therefore, we need to evaluate how other kinds of security attacks can affect cognitive radio networks. For example, if we know that the secrecy capacity between two nodes is small, then we need to further strengthen the security mechanisms to defend against the potential security attacks.

Conclusion

In this article, we investigated the security issues related to the physical layer in cognitive radio networks. First, we summarized the security attacks on the physical layer for cognitive radio networks and surveyed the existing countermeasures for those attacks. We further presented a cognitive radio network model to analyze the secrecy capacity of the network. The performance results helped to characterize the secrecy capacity and outage probability between a node and its neighbors, which can give an upper bound on how much secure information can be transmitted in cognitive radio networks. The secrecy capacity analysis can help us to determine how secure a cognitive radio network is and whether we need to further strengthen the security mechanisms to defend against the potential attacks in the cognitive radio networks.

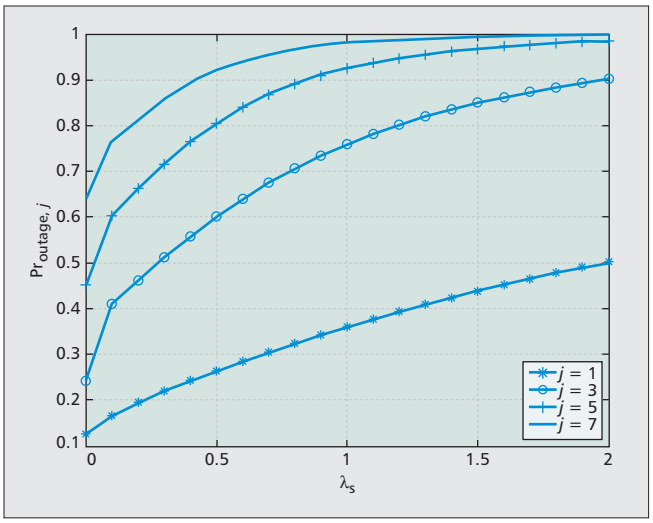

Figure 4. *Outage probability of secrecy capacity* $C_s(i, j)$ *for various values of* j ($R_s = 1$).

Acknowledgement

This work was supported in part by NSF grant CNS-1065069.

References

[1] I. F. Akyildiz *et al.*, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey," *ACM Int'l. J. Computer and Telecommun. Net.*, vol. 50, issue 13, Sept. 2006, pp. 2127–59.

[2] B. Konings, "PHY and MAC Layer Security in 802.11 Networks," http://www.uni-ulm.de/fileadmin/website_uni_ulm/iui.inst.100/ institut/mitarbeiter/koenings/koenings_thesis_summary.pdf.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 24, no. 4, July 1978, pp. 451–56.

[4] H. Khodakarami and F. Lahouti, "Link Adaptation for Physical Layer Security Over Wireless Fading Channels," *IET Commun.*, vol. 6, issue 3, 2012, pp. 353–62.

[5] O. Leon, J. H. Serrano and M. Soriano, "Securing Cognitive Radio Networks," *Int'l. J. Commun. Systems*, vol. 23, 2010, pp. 633–52.

[6] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," *J. Internet Tech.*, vol. 12, no. 2, 2011, pp. 25–37.

[7] R. Chen, J. M. Park, and J. H. Reed, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE JSAC*, vol. 26, issue 1, 2008, pp. 25–37.

[8] T. C. Clancy, and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," *IEEE Crowncom*, May. 2008, pp. 1–8.

[9] R. Chen *et al.*, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," *IEEE Commun. Mag.*, vol. 46, no. 4, 2008, pp. 50–55.

[10] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel Jamming Attacks using Cognitive Radios," *IEEE ICCCN*, Aug. 2007, pp. 352–57.

[11] W. Xu *et al.*, "Channel Surfng and Spatial Retreats: Defenses Against Wireless Denial of Service," *Proc. 3rd ACM Wksp. Wireless Security*, Philadelphia, PA, Jan. 2004, pp. 80–89.

[12] L. Zhang *et al.*, "On the Relationship Between the Multi-Antenna Secrecy Communications and Cognitive Radio Communications," *IEEE Trans. Commun.*, vol. 58, issue 6, June 2010, pp. 1877–86.

[13] Z. Shu *et al.*, "Impact of Interference on Secrecy Capacity in a Cognitive Radio Network," *Proc. IEEE Globecom 2011*, Houston, TX, Dec. 2011.

[14] J. Kingman, *Poisson Processes*, Oxford University Press, 1993.

[15] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

Biographies

ZHIHUI SHU [S'10] (zshu@unomaha.edu) received a BE degree from Wuhan University, Wuhan, China, in 2006 and a ME degree from Shanghai Jiao Tong University, China, in 2010, respectively. In August 2010, he joined University of Nebraska-Lincoln, as a Ph.D. student. His current research interests include cognitive radio networks, wireless security, and smart grid communication systems.

YI QIAN [M'95, SM'07] (yqian@ieee.org) received a Ph.D. degree in electrical engineering from Clemson University. He is an associate professor in the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln (UNL). Prior to joining UNL, he worked in the telecommunications industry, academia, and the government. Some of his previous professional positions include serving as a senior member of scientific staff and a technical advisor at Nortel Networks, a senior systems engineer and a technical advisor at several start-up companies, an assistant professor at University of Puerto Rico at Mayaguez, and a senior researcher at National Institute of Standards and Technology. His research interests include information assurance and network security, network design, network modeling, simulation and performance analysis for next generation wireless networks, wireless ad-hoc and sensor networks, vehicular networks, broadband satellite networks, optical networks, high-speed networks and the Internet. He has a successful track record to lead research teams and to publish research results in leading scientific journals and conferences. Several of his recent journal articles on wireless network design and wireless network security are among the most accessed papers in the IEEE Digital Library. He is a member of ACM.

SONG CI [S'98, M'02, SM'06] (sci@engr.unl.edu) received his B.S. from Shandong University of Technology (now Shandong University), Jinan, China, in 1992, M.S. from Chinese Academy of Sciences, Beijing, China, in 1998, and Ph.D. from the University of Nebraska-Lincoln in 2002, all in Electrical Engineering. Currently, he is an Associate Professor of Computer and Electronics Engineering at the University of Nebraska-Lincoln. His research interests include: dynamic complex system modeling and optimization, green computing and power management, dynamically reconfigurable embedded system, cognitive network management and service-oriented architecture.