International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 17 Issue 2 – SEPTEMBER 2015.

ANALYSIS AND COUNTERFEITING OF PHYSICAL LAYER ATTACKS IN COGNITIVE RADIO NETWORKS

Mr.Malleshwar[#1], Prof.Mr.S.SRINIVAS[*2]

[#1]*Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Shamshabad, Telagana INDIA*

[*2]*Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Shamshabad, Telagana INDIA*

mallesh2@outlook.com
s.srinivas@vardhaman.org

***Abstract*—In this paper, we study the denial-of-service (DoS) attack and physical layer attack on secondary users in a cognitive radio network by primary user emulation (PUE). Most approaches in the literature on primary user emulation attacks (PUEA) discuss mechanisms to deal with the attacks but not analytical models. This paper considers physical layer attacks, primary user emulation attacks (PUEA) and routing attacks in cognitive radio networks operating in the white spaces of the digital TV (DTV) band. We propose a reliable ECC scheme, in which the network validates the nodes by verifying the authentication reference signals. The proposed model uses digital authentication to validate the receiver node. Then the model organizes a physical data distribution to the receiver. During the validation the proposed model computes the data for avoiding data leakages. The proposed model allows transmitter and receiver to share secrete signals by distributing reference keys to achieve accurate identification of authorized primary users. We deploy the Cognitive radio model in NS2 2.31and we analyze the network performance against different kind of attacks.**

Keywords*— *Cognitive radio, security, primary user emulation attack, energy detection, elliptic curve cryptography

I. INTRODUCTION

Communication is a transfer of information from one point to another. Today's communication is very advance; we use many new technologies like Cognitive radio network is latest one. The term Cognitive Radio was first officially presented by Mitola and Maguire in 1999 [1].Cognitive radio network is a network in which an un-licensed user can use an empty channel in a spectrum band of licensed user. Cognitive Radio Networks (CRNs) is an intelligent network that adapt to changes in their network to make a better use of the spectrum. CRNs solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference. Generally licensed users are known as primary users and un-licensed users are secondary users. When information is send through a licensed spectrum band is a primary user, only some channel of band is used, others are empty.

Among all the key technical problems of CR networks, security is a crucial but not well addressed issue. Due to the nature of dynamic spectrum access and the fact that the CR network should not interact with the primary network, the SU s in the CR network usually lack global information about the usage of the spectrum resource in the network. This makes the CR network vulnerable to attacks by hostile users. In all the main functionalities of CR networks such as spectrum sensing, spectrum mobility, spectrum sharing and spectrum management, the CR network has been shown to be strategically vulnerable [1]. The typical attacks on CR networks may include Denial of Service (DoS) attacks, system penetration, repudiation, spoofing, authorization violation, malware infection, and data modification. These attacks cause potential threats to the information confidentiality, integrity and availability of the CR network. Effective defense approaches are urgently needed to secure CR networks and deal with these attacks. Nowadays, security threats and their countermeasures have been studied as one of the most important topics in the research area of CR technology [6].

PUEA in cognitive radio networks was studied in [8],[9],[10]. In [8], Chen and Park propose two mechanisms to detect a PUEA namely the distance ratio test (DRT) and the distance difference test (DDT), which use the ratio and the difference, respectively, of the distances of the primary and malicious transmitters from the secondary user to detect a PUEA. In [9], Chen et al discuss defense against PUEA by localization of primary transmitters. Directional antennas were proposed to determine the angle of arrival of the primary signal, and using this, the time of arrival and the received signal strength, the secondary users determine the location of the primary transmitter. A different kind of threat albeit not directly a PUEA, was discussed by Chen et al in [10]. The authors consider a system where spectrum sensing is done and a hypothesis testing method is used to detect a transmission,

which in the case of cognitive radio networks could be a primary transmission. A Byzantine failure model due to fraudulent reporting of spectrum sensing was discussed and a weighted sequential ratio test was proposed to overcome this attack. In most approaches, the detection of PUEA depends on the determination of the location of the primary transmitter, which, in turn, depends on the direction of signal arrival. The dependence on the directionality of the antennas at the receiver makes the detection process complex because most of the incumbent receivers in wireless and cellular networks use omni directional antennas

In this paper, we mainly focus on the security problem arising from Primary User Emulation (PUE) attacks in CR networks. PUE attacks are known as a new type of attacks unique to CR networks. In such an attack, the hostile user takes the advantage of the inherent etiquette in CR networks that the legitimate SU has to evacuate the spectrum band upon the arrival of a PU. An attacker emulates the PU's transmitting signal and misleads the legitimate SU to give u p the spectrum band. The presence of PUE attacks may severely influence the performance of CR networks. This paper aims at presenting a comprehensive introduction to PUE attacks, from the attacking principle and its impact on CR networks, to the detection and defense approaches. In order to secure C R networks, we propose a database-assisted detection approach and an admission control based defense approach against PUE attacks

We propose a solid AES-helped DTV plan, where an AES-scrambled reference sign is created at the TV transmitter and utilized as the sync bits of the DTV information outlines. By permitting a common mystery between the transmitter and the collector, the reference sign can be recovered at the recipient and used to accomplish exact identification of approved essential clients. Additionally, when joined with the investigation on the auto-connection of the got signal, the presence of the malevolent client can be distinguished precisely regardless of the essential client is available or not. The proposed methodology can viably battle PUEA with no adjustment in equipment or framework structure aside from of a module AES chip, which has been popularized and generally accessible

II. COGNITIVE RADIO

Cognitive Radio (CR) is a novel technology that promises to solve the spectrum shortage problem by allowing secondary users to coexist with primary users without causing interference to their communication. Although the operational aspects of CR are being explored vigorously, its security aspects have gained little attention. In this paper, a brief overview of the CR technology is provided followed by a detailed analysis of the security attacks targeting Cognitive Radio Networks (CRNs) along with the corresponding mitigation techniques. We categorize the attacks with respect to the layer they target starting from the physical layer and moving up to the transport layer. An evaluation of the suggested countermeasures is presented along with other solutions and augmentations to achieve a secure and trusted CRN.

Cognitive Radio (CR) nodes have unique capabilities which allow them to take advantage of available white spaces in a spectrum. A study made at the Berkeley Wireless Research Center (BWRC) shows that most spectrum, particularly from 1 GHz to 10 GHz is underutilized, as shown in Figure 1. The nodes can sense their environment and spectrum, analyze the discovered information, and adjust to the sensed environment. CR nodes discover white spaces by performing spectrum sensing; the ability to identify or detect holes in a spectrum. The techniques used to make use of these holes fall under the term Dynamic Spectrum Access (DSA). The Two most significant challenges in CRNs are: Transparency to primary users and non-interference.

2.1 Cognitive Radio Networks: Attacks and Countermeasures

Unlike most of the surveys that address the attacks on CRNs, we categorize the attacks according to the layers they target: Physical, Link, Network, and Transport. Since CRNs can be considered a special kind of Ad Hoc network, most of the attacks targeting Ad Hoc networks can also target CRNs. In this survey, we analyze the attacks that are most relevant to CRNs. It is important to note that there already exist some surveys on CRNs [12-13], but they have many weaknesses in the sense that they miss to address some very important attacks, they are outdated, and most importantly none presents an evaluation study of the various countermeasures. Any solution suggested to counter CRN attacks should abide by the FCC requirement which states that "no modification to the incumbent system should be required to accommodate opportunistic use of the spectrum by secondary users" [14]. Having this requirement in mind, any security solution suggested to protect or thwart an attack on CRN should be introduced to the secondary user system, not the primary one.

2.2 Physical **Layer Attacks**

Before discussing the physical layer attacks on CRN and the corresponding countermeasures, we highlight the work done in [15] that addresses the physical-layer security issue of a secondary user in CRN from an information theoretic perspective where a secure multiple-input single output (MISO) cognitive radio channel was considered. In MISO, a multi-antenna SU transmitter sends confidential information to a legitimate SU receiver in the presence of an eavesdropper and on the licensed band of a primary user (PU). The approach defines the Secrecy Capacity as the maximum achievable rate at which the data can be reliably sent from the SU transmitter to the legitimate SU receiver but is kept perfectly secret from Eavesdropper. The secrecy capacity of a secure MISO CR channel has been characterized. Two numerical approaches have been proposed to compute the secrecy capacity and the capacityachieving transmit covariance matrix. By exploring the inherent convexity, the first approach has transformed the

original quasiconvex problem into a single semi definite program by exploring its inherent convexity, which can be solved efficiently. By exploring the relationship between the secure CRN with the conventional CRN, the second approach has transformed the original problem into a sequence of optimization problems related to the conventional CRN. 4.1.1 Primary User Emulation (PUE) One of the Cognitive Radio principles is that a secondary user is allowed to use a specific band as long as it's not occupied by a primary user. However, once the secondary user detects the presence of a primary user, it must switch channels immediately to an alternative band in order not to cause interference to the primary user. If the secondary user detects another secondary user using the same band, certain mechanisms should be used to share the spectrum fairly. Primary User Emulation (PUE) attack [14][16] is carried out by a malicious secondary user emulating a primary user or masquerading as a primary user to obtain the resources of a given channel without having to share them with other secondary users .

As a result, the attacker is able to obtain full bands of a spectrum. The motivation behind the attack is divided into two categories: Selfish PUE attack and Malicious PUE attack. In the Selfish PUE attack, the attacker's goal is to increase its share of the spectrum resources. In addition, this attack can be conducted simultaneously by two attackers to establish a dedicated link between them. In the Malicious PUE attack, the attacker's goal is to prevent legitimate secondary users from using the holes found in a spectrum. Data collector (Fusion center) Sensing Terminals Sensing Terminals Sensing Terminals Local Spectrum Sensing Results Signals with the same characteristics as Primary User signals Primary User Final spectrum sensing result Data Fusion Malicious user.

Primary User Emulation Attack The PUE attack can target both types of cognitive radio Policy Radios and Learning Radios [1] with different severity. When dealing with policy radios, the effect of the attack vanishes as soon as the attacker leaves the channel. The secondary user will then sense that the spectrum is idle and claim it. On the other hand, when dealing with learning radios, information about primary users' current and past behavior can be gathered in order to predict when they will leave the channel, i.e., make it idle. The attacker can then perform the PUE attack during these idle times. Now the attack will have a long term effect on secondary users and they might never use the affected channel ever again.

As mentioned in [12], new and more sophisticated PUE attacks can be performed when having some knowledge about the cognitive radio network. For instance, an attacker can utilize the CRN's "quiet periods" to perform PUE attacks. A quiet period is the time during which all secondary users refrain from transmitting to facilitate spectrum sensing. During these periods, any user whose received signal strength is beyond a certain threshold is considered a primary user. This CRN feature can be exploited by an attacker who transmits during "quiet periods" fooling the rest of the nodes as being a primary user. Another example is an attacker that performs new PUE attacks whenever the CRN makes a frequency handoff, i.e., switches from one channel to another, thus degrading the data throughput of the CRN or completely leading to DoS. Such an attack assumes that the attacker can find the next CRN in a limited time. Apart from the experimental PUE attacks, an analytical model is described in [17] to obtain the probability of successful PUE attacks on secondary users.

The authors provided lower bounds on the probability of a successful attack using Fenton's approximation and Markov inequality. We discuss next the approaches used to thwart PUE attacks. y Defending Against Primary User Emulation Attack To defend against PUE attacks, the identity of the transmitting source needs to be identified, i.e., is the transmitting source a primary user or a malicious user? The usual and best approach of knowing the user identity is to apply cryptographic authentication mechanisms, such as digital signatures. But such an approach cannot be adapted because of the FCC regulation that prohibits altering primary user systems. Given this restriction and knowing that primary users' locations are known ahead of time, researchers resorted to finding efficient ways of pin pointing the location of the transmitting source.

III. Detecting the PUE Attack

3.1. Overview of the Approach In the remainder of the paper, we call the sender whose position we try to locate as the interested sender (it could be the primary user or an emulator), and the sender of the interfered signals as the reference sender. The PNC based localization technique provides a very promising approach to distinguishing the real primary user from an emulator: when an unknown signal is detected, a legitimate secondary user can intentionally send out a sequence to interfere with the signal. Other secondary users can capture the interference results and determine the hyperbolas. If the intersection point of the hyperbolas is at the known position of the primary user, the secondary users will leave the channel.

Otherwise, they will stay there. The major challenge that we face is the safety of the approach. Since we cannot distinguish an attacker from a legitimate secondary user, the attackers can participate in the localization procedure. They can send out false information about their positions and interference results to mislead the calculation procedures. Therefore, we must design mechanisms to defend against such attacks. In the following scenario, we assume that trustworthy reference senders exist in the network. This scenario matches the application environments of the IEEE 802.22 [12] and 802.16h [13] network standards. The trustworthy nodes can serve as the reference senders during PUE detection. We assume that the signals from a trustworthy sender TR can be correctly received by p legitimate secondary users {s1, s2, · · ·, sp} and q attackers {m1, m2, · · ·, mq}.

At the same time, we also assume that all these nodes can correctly receive the signals from the real primary user P. When TR senses the communication channel and detects some signals that could have come from the real primary user, it will initiate the PUE detection procedure. TR will choose a random number as the seed for the PRBG to generate a random bit sequence and use the sequence to fill a data packet. When it sends out the packet, the radio waves from TR will interfere with the signals from the primary user (or an emulator). Message authentication codes (MAC) will be attached to the packets to protect their authenticity and integrity. The details of the MAC codes will be discussed later. Using the mechanism described in [11, 14], the wireless nodes can detect the signal collision and record the interference results. Using the MAC code from TR, they can verify the identity of the sender and integrity of the information.

They will then use the PRBG to regenerate the random sequence. Combining the interference results with the regenerated sequence, the receivers can recover the packet from the interested sender. The receivers can then calculate the values based on the starting points of interference and the frequency of the radio signals. Now every receiver (both legitimate secondary users and attackers) will exchange its position, and the hash result of the recovered packet from the interested sender with its neighbors. The broadcast packets will be protected by the MAC codes so that the receivers can verify their contents. The secondary users can combine the values with the node positions to determine the position of the interested sender. Once the position is determined, secondary users can compare it with the known position of the primary user to determine whether or not they are under a PUE attack

3.2 Prevention against Physical layer attacks

Two approaches have been suggested to prevent our network to PUE attack on physical layer: Distance Ratio Test (DRT) which is based on received signal strength measurements and Distance Difference Test (DDT) which is based on signal phase difference. [5].Both approaches are based on a transmitter verification procedure. Defending against jamming attack, we use CSMA (carrier sensing multiple access) in which a device will continuously sense a channel until it finds to be empty. A jamming detection technique that investigates the relationship between Signal Strength (SS) and Packet Delivery Ratio is suggested. [5]
PHY Layer Attack Model As discussed in Section II, malicious users can report false sending data to the common receive (i.e. fusion center) such that they can mislead the results of collaborative spectrum sensing. For example, an attacker can report high energy level when the actual sensed energy is low. If the fusion result by the common receiver is on (primary user is present), the attack is successful Before demonstrating the RFSD attack model, we review the characteristics of sensing reports from honest secondary users. Let Ei denote the sensing energy for the i th cognitive user in each sensing period, the distribution of Ei

IV. SECURITY ANALYSIS OF THE PROPOSED AES-ENCRYPTED

AES is a robust symmetric-key cipher, in which a single key is used for both encryption and decryption. The key is shared between the transmitter and the receiver and is kept private shows the general structure of the AES encryption algorithm. It mainly consists of four stages that are applied to the input data, which is arranged in 4 X 4 array of bytes. The four stages are repeated, and the number of repetition depends on the key length. The four stages of AES are:

1) SubBytes Stage In this stage, each byte in the 4 X 4 array is simply mapped to another byte based on a lookup table called the S-box. The security reason for creating the S-box is to thwart all the known cryptanalytic attacks [9].

2) ShiftRows Stage Here, each row in the 4 X 4 data array, except the first row, is shifted to the left by a number of bytes. In particular, the second row is shifted to the left by 1 byte, while the third and fourth are shifted by 2 bytes and 3 bytes, respectively. The ShiftRows stage provides diffusion in the cipher so that the output of the AES algorithm (i.e. the ciphertext) carries no statistical relationship to the input (i.e. the plaintext) [9].

3) MixColumns In this stage, each byte in a column is replaced by a combination of the fours bytes within the same column. The MixColumns operation also provides diffusion property [9].

4) AddRoundKey In this stage, each byte in the array is added to the RoundKey array using bit-wise XOR function. The AddRoundKey stage is used to impact every bit within the array [9]. It has been proved that AES is secure under all known attacks [9]. More specifically, it is computationally infeasible to break AES.

4.1 Security of the AES-encrypted

The AES algorithm has a very important security feature, besides the above, known as the avalanche effect. The avalanche effect means that a small change in the plaintext or the key yields to a large change in the ciphertext. Because of the avalanche effect of the AES algorithm, if two random plaintexts are applied to AES algorithm, the resulting ciphertexts will have approximately 50% correlation [9]. Actually, even if one bit is changed in the plaintext, the correlation in the ciphertext will be approximately 50%. To illustrate the security of the AES-encrypted DTV based on the avalanche effect, we obtain the cross-correlation between different malicious signals and the reference signal.

4.2 Elliptic curve cryptography Authentication process

The authentication process for each of the member in the group. The authentication process starts with the generation of threshold signature using ECC model.
The network consist of the following parameters:

- Server (S)
- A set of Member Node X = {N1……N_{S2}) where N_{S2} represents identity of the ith $(1 \le i \le S1)$ member.
- A set of signer $Y = \{K1, \ldots\ldots K_{S2}\}$ where K is a subset of N and K_{S2} represents the identity of the jth ($1 \le i \le S2$) member
- Verifier V

In order to generate a threshold signature for hello message m performs the following steps

Step 1: In the first step, all the member node request for threshold signature. This is started by one of the signers by sending a threshold generation request to Server S along with list of signers as (TK1… TK_{S2}).
Step 2 : In the next step they sends tokens. For this server selects a random token $T_R \in Z^*_q$ whe $(1 \le R \le S_2)$ and sends them to the corresponding signers very securely.
Step 3: After that each signer creates a signature: $Sig_{PK_R} = H_0(N).K_{PK_R}$ and calculates with a corresponding token: $T \cdot Sig_{PK_R} = TA \cdot Sig_{PK_R}$
Step 4: After that sender sends hello packet with signature to receiver. Here, reciever sends the message packet to the Server.
Step 5: Server verifies the sender packet and validates signature

4.3 Authentication protocol procedure

Step1: The sender device need to access the receive nodes, it will generate a random number r1.
Step2: Calculate the requesting code Rc
Step3: Pass requesting code to receiver as request
Step4 : Initiate the verification of authentication of the corresponding Senders
Step5: To achieve this the receiver node will generate a random number r2 and send it to sender
Step6: The sender will generate authentication-verifying code AVc as a response
Step7: This AVc will be sent to the receiver node for its authentication verification
Step8 : If the above condition is satisfied, the receiver node will come for a conclusion that the sender node is a valid one
Step9: The condition will be satisfied only if the private key, public key and the generating point are same

V. Implementation and Evolution

We evaluate the performance of proposed model through NS2. We design a network with a range of 1000*1000 sqm, we configure a nodes by placing all these nodes on selected region. Here we consider different number of nodes , we assign different energy rate level and transmission range level. We consider bandwidth as 1Mbps and we have evaluated the proposed approach to evaluate a results . Here we create four different modules to organize communication

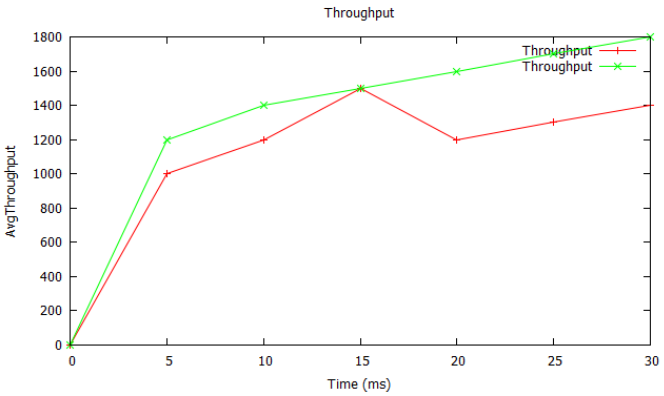

Fig1: Throughput

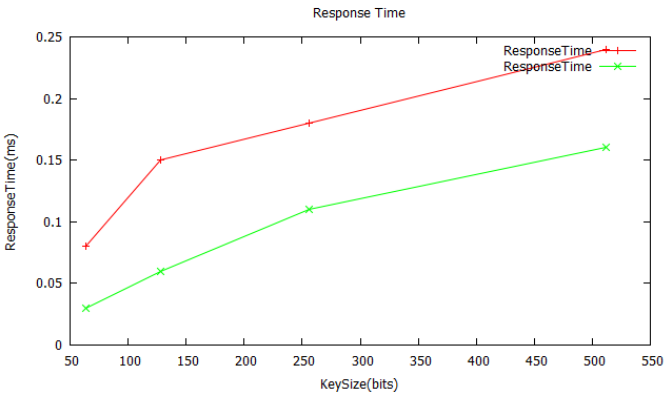

Fig 2: Response Time

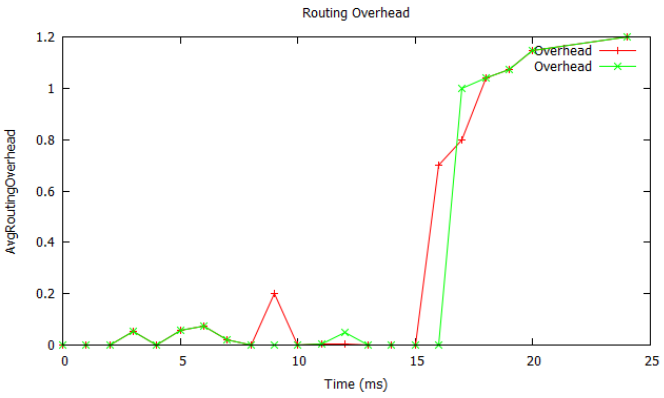

Fig 3: Routing Overhead

VI. CONCLUSION

In this paper, we propose advanced Eliptic curve cryptography model for to identify the malicious before disturbing physical signals to the receiver end. In this process the detection model validates the nodes before initiating physical data communication which leads to the better network performance and reduces the network overhead. In this paper we have researched various attacks and attacks process to identify the attack level at different spectrum bands. We have configured the Cognitive radio network model by enriching the ECC application during transmitting singles to receiver. The ECC model validates each node authentication by validating hello packets, and it verifies its authentication codes. We have done simulation for analyzing network performance, we compare the performance by considering response time, routing overhead and throughput. We enhance this study on different spectrum radio model for preventing eavesdropping attacks.

REFERENCES

[1] Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, and Tongtong Li, Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard, IEEE, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 5, MAY 2014

[2] Mitola III J, Maguire Jr G. Cognitive radio: making software radios more personal. Personal Communications, IEEE [see also IEEE Wireless Communications] 1999; 6(4):13–18. DOI: 10.1109/98.788210.

[3] Simon Haykin, Life Fellow, IEEE. Cognitive Radio: Brain-Empowered Wireless Communications IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 2, FEBRUARY 2005

[4] Towards Secure Cognitive Communications in Wireless Networks Tingting Jiang, Virginia Tech Tongtong Li and Jian Ren, Michigan State University

[5]Survey of Security Issues in Cognitive Radio Networks Wassim El-Hajj1, Haidar Safa1, Mohsen Guizani2,
Journal of Internet Technology Volume 12 (2011) No.2

[6] T. Charles Clancy and Nathan Goergen, Security in Cognitive Radio Networks: Threats and Mitigation, International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), Singapore, May, 2008, pp.1-8.

[7] Rajesh K. Sharma and Jon W. Wallace, *Improved Spectrum Sensing by Utilizing Signal Autocorrelation*, *Proceedings of IEEE Vehicular Technology Conference*, Barcelona, Spain, April, 2009, pp.1-5.

[8] Ruiliang Chen, Jung-Min Park and Jeffrey H. Reed, *Defense against Primary User Emulation Attacks in Cognitive Radio Networks*, *IEEE Journal on Selected Areas in Communications*, Vol.26, No.1, 2008, pp.25-37.

[9] Huahui Wang, Leonard Lightfoot and Tongtong Li, *On PHY-Layer Security of Cognitive Radio: Collaborative Sensing under Malicious Attacks*, *44th Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March, 2010, pp.1-6.

[10] Eric Wong and Rene Cruz, *On Physical Carrier Sensing for Cognitive Radio Networks*, *Forty-Fifth Annual Allerton Conference on Communication, Control, and Computing*, Allerton House, UIUC, IL, September, 2007.

[11] Bertrand Mercier, Viktoria Fodor, Ragnar Tobaben et al., *Sensor Networks for Cognitive Radio: Theory and System Design*, *ICT Mobile Summit*, Stockholm, Sweden, June, 2008.

[12] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[13] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[14] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, 2009.

[15] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2135–2141, Jul. 2011.

[16] C. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. 4th IEEE CCNC*, Jan. 2007, pp. 1037–1041.

[17] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Proc. IEEE ICASSP*, May 2013, pp. 2935–2939.

[18] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surv. Tuts.*, vol. 15, no. 1, pp. 428–445, Mar. 2013.

[19] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symp. SP*, May 2010, pp. 286–301.

[20] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede, "A 3.84 Gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology," in *Proc. 15th ACM Great Lakes Symp. VLSI*, New York, NY, USA, 2005, pp. 60–63.