ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

PRIMARY USER AUTHENTICATION IN COGNITIVE RADIO NETWORKS: A SURVEY

T.Lakshmibai[1], B.Chandrasekaran[2], C.Parthasarathy[3]

Research Scholar, Dept. of ECE, SCSVMV UNIVERSITY, Kanchipuram, Tamilnadu, India [1]

Asst.Professor, Dept. of ECE, SCSVMV UNIVERSITY, Kanchipuram, Tamilnadu, India [2]

Asst.Professor, Dept. of IT, SCSVMV UNIVERSITY, Kanchipuram, Tamilnadu, India [3]

ABSTRACT: For effective usage of radio frequency spectrum, cognitive radio networks have been proposed, allowing the secondary users to occupy the spectrum whenever the primary user is not using it. To avoid interference with the primary user secondary user should constantly check the usage of the spectrum. But achieving a faithful monitoring is not so easy. Hence Primary user Emulation (PUE) attack comes into existence. To counter this attack primary user's signal can be authenticated in the physical layer itself. In this paper, we provide various approaches (dealt in different papers) for authenticating primary users' signals that conforms FCC's requirement.

Key words: Cognitive Radio (CR), PUE attack, Primary User (PU), Secondary User (SU).

I – INTRODUCTION

Today's wireless networks are based on Fixed Spectrum Assignment Policy. In this the actual utilization of the spectrum is only about 15% to 85% of the assigned, at any point of time. The inefficiency of spectrum usage and limitations in the availability of spectrum necessitates a new communication paradigm called Cognitive Radio networks. Cognitive Radio (CR) is a form of a wireless communication which detects which of the communication channels are in use and which are not in use and immediately occupies the vacant channels leaving the occupied ones.

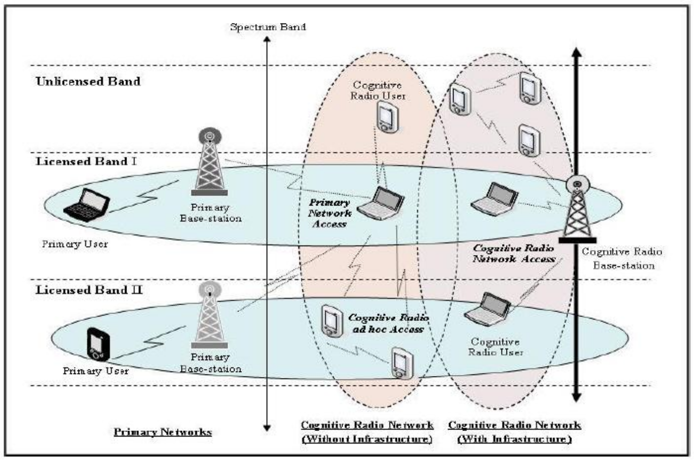
II - COGNITIVE RADIO NETWORK

COGNITIVE RADIO ARCHITECTURE

The Cognitive radio network architecture shown below comprises of two network groups namely Primary network and Cognitive radio network.

Primary Network: An existing network infrastructure is called Primary network. The user in this network (Primary users) has rights to operate certain spectrum of band called licensed band. The examples of this network are Television Broadcasting network and cellular communication networks.

Cognitive Radio Network: Otherwise called a Secondary network which does not have any desired band to operate and thus it operates in the unlicensed band.



(courtesy of http://3g4g.blogspot.com/2007_06_01_archive.html)

Figure 1. **Cognitive Radio Architecture**

Cognitive radio users can either communicate with each other in a multihop manner or can access the base-station. The three different access types over heterogeneous networks used in the cognitive radio network architecture are:

1. Cognitive Radio Network Access: Cognitive radio users can access their own cognitive radio base-station both on licensed and unlicensed spectrum bands. Since all the communications occur within the cognitive radio network, their medium access scheme is independent of that of primary network.

2. Cognitive Radio AdHoc Access: Cognitive radio users can communicate with each other through ad hoc connection on both licensed and unlicensed spectrum bands. Also cognitive radio users can have their own medium access scheme.

3. Primary Network Access: The cognitive radio user can access the primary base-station through the licensed band, if the primary network permits. Unlike other access types, cognitive radio users should support the medium access technology of primary network. Also, primary base-station should support cognitive radio capabilities.

COGNITIVE RADIO FUNCTIONS

CR technique enables the users to have the “Best available channels”

Spectrum sensing – Detects unused spectrum and share the spectrum without harmful interference with other users.
Spectrum Management – Select best available channel
Spectrum Sharing – Coordinate access to this channel with other users.
Spectrum Mobility – Vacate the channel when licensed user is detected.

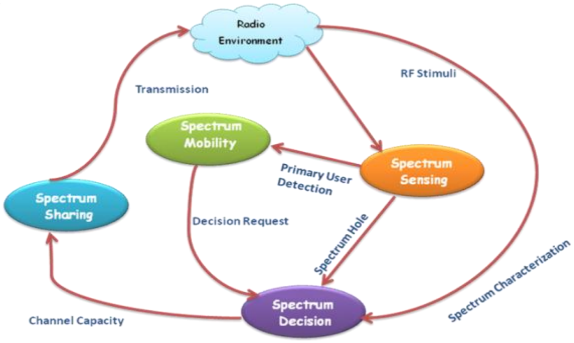


Figure 2 Cognitive Cycle.

Cognitive Radio Network Applications:

Cognitive Radio Networks are used in Emergency network, Military network, CR Mesh Network, Leased Network, Cellular Network and in Multimedia.

III - PUE ATTACK

Security threat to CR is Primary User Emulation (PUE) attack. Because of inefficient usage of frequency spectrum, CR networks are proposed. The basic idea is allowing secondary users to use a spectrum if the primary user is not using it. To achieve this, each secondary user must monitor the usage of the spectrum to avoid interference with the primary user. This imposes problems in the efficient and trustful monitoring of the usage. A malicious secondary user who wants to gain an unfair use of the spectrum can emulate the primary user, and can thus trick the other secondary users in to believing that the primary user is using the spectrum when it is actually not.

This is called PUE (Primary User Emulation) attack. To prevent this attack there should be a way to authenticate primary user's spectrum usage.

IV - DETAILED STUDY

To counteract the PUE attack, a transmitter verification scheme [1], called *LocDef (localization based defense)*, is used to verify whether the given signal is from an incumbent transmitter by estimating its location and observing its signal characteristics. This can be integrated into the spectrum sensing process and LocDef employs a *non-interactive localization* scheme to detect and pinpoint PUE attacks under certain conditions.

For authenticating primary users' signals [2] that conforms to FCC's requirement is a novel approach which integrates cryptographic signatures and wireless link signatures. Here the helper node serves as a "bridge" to enable a secondary user to verify cryptographic signatures carried by the helper node's signals and then obtain the helper node's authentic link signatures to verify the primary user's signals. With the proximity of the helper node to the primary user it does not require any training process.

The identification of attacks on Physical-layer [3] the modulation-based and transient-based fingerprinting techniques are performed.

In Transient-based technique, the unique features are observed when the radio is turned on during transient phase. These features appear at the beginning of each packet transmission as shown in Figure 3. It is used for distinguishing classes (e.g., model and manufacturer) of wireless devices

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2014

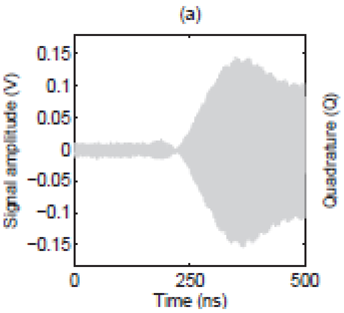


Figure 3

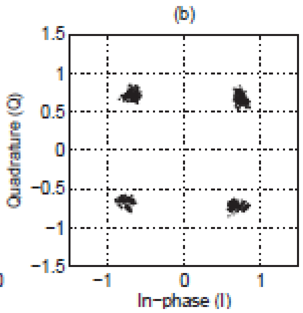


Figure 4

Modulation-based techniques rely on imperfections in the modulator of the radio transceiver such as frequency and constellation symbol deviations (Figure 4).The modulation-based features are vulnerable to feature and signal replay, whereas transient-based identification is vulnerable to signal replay attacks.

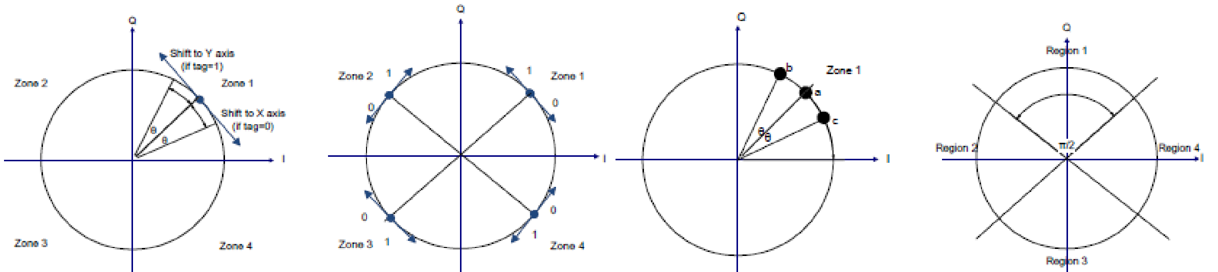
For spectrum usage authentication using cryptographic link signature [4], eliminates the need for helper nodes as in [2]. Here there are two schemes to add a signature, one using modulation, and the other using coding can be used. The primary user detection, (i.e. to detect whether a primary user is using its spectrum or not) approaches are 1. Energy detection and

2. Feature detection

In energy detection, secondary users use energy strength to identify a primary user's signal, whereas in feature detection, secondary users find some specific features of a signal, and use these features to identify a primary user.
Examples of features include pilot, synchronization word and cyclostationarity. In this authentication scheme, authentication tags are first generated and then transmitted.

ADDING TAGS TO MODULATION

The authentication tags can be transparently added to modulation schemes at the physical layer. Tags are added as noise.



(a) Phase Shifting (b) Shifting Directions (c) An Example (d) Tag Detection Regions

Figure 5: The QPSK Tagging Scheme

The tags (man-made noise) to QPSK are to perturb the position of the phase in the constellation diagram.

When the tag is 1, we shift the phase by θ degree towards the y-axis, where $0 < \theta < \Pi/4$. The final position stays on the circle to maintain the same signal energy.

When the tag is 0, we shift the phase by θ degree towards the x-axis.

ADDING TAGS TO CODING

The authentication tags can be transparently added to the coding module at the physical Layer called Error Correcting Code (ECC).

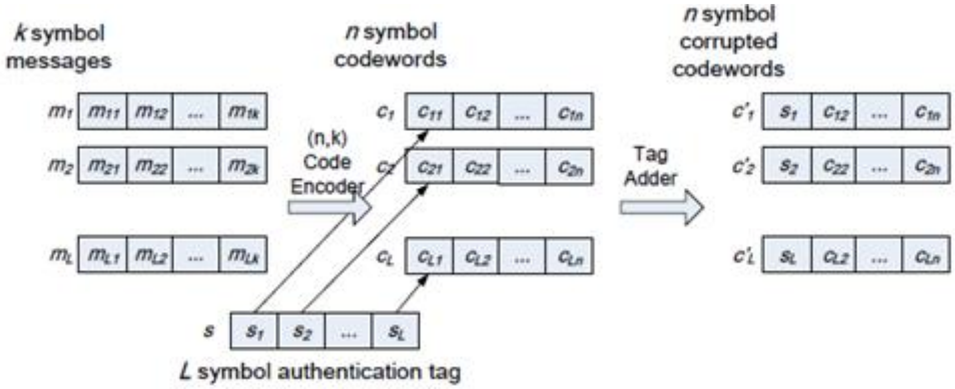

k symbol messages
n symbol codewords
n symbol corrupted codewords
m_1 m_{11} m_{12} ... m_{1k}
m_2 m_{21} m_{22} ... m_{2k}
m_L m_{L1} m_{L2} ... m_{Lk}
(n,k) Code Encoder
c_1 c_{11} c_{12} ... c_{1n}
c_2 c_{21} c_{22} ... c_{2n}
c_L c_{L1} c_{L2} ... c_{Ln}
Tag Adder
c'_1 s_1 c_{12} ... c_{1n}
c'_2 s_2 c_{22} ... c_{2n}
c'_L s_L c_{L2} ... c_{Ln}
s s_1 s_2 ... s_L
L symbol authentication tag

Figure 6: The ECC Tagging Scheme

Primary user authentication system for mobile cognitive radio networks [5] was performed with low power helper nodes. This system relies on a combination of physical-layer signatures (link signatures) and cryptographic mechanisms to reliably sense PU activity and relay information to the CRN. The mobile secondary users were accommodated in this system without the need for repeated training with every location change.

The security issues and PHY-layer Authentication for Transmitter Identification [6] is proposed in this scheme. The multipath indoor office scenario with time-invariant propagation channel was considered, and the transmitter location fingerprints are extracted from wireless medium. Wavelet transform is used to magnify the characteristics of transmitter fingerprints.

For defeating PUE attack [7], Belief propagation is used, which avoids the deployment of additional sensor networks and expensive hardware used in networks. Each secondary user calculates the local function and the compatibility function, computes the messages, exchanges messages with the neighboring users, and calculates the beliefs until convergence. Then PUE attacker will be detected, and all the SUs in the network will be notified in a broad cast way about the characteristics of the attacker's signal. Thus all SUs can avoid the PUE attacker's primary emulation signal in future.

In Physical layer authentication [8], the authentication information is transmitted concurrently with the data. Without any additional bandwidth authentication is added with carefully designed secret modulation on the waveforms. But it increases the probability of data recovery error. However, with a long enough authentication codeword, a useful authentication can be achieved with very slight data degradation. Also, by treating the authentication tag as a sequence of pilot symbols, the data recovery can actually be improved by the aware receiver.

A novel QoE-driven channel allocation scheme for [9] SUs and cognitive radio networks (CRN) base station (BS) is proposed. The QoE(Quality of Experience) data under different primary channels (PCs) are collected by the SUs and delivered to a Cognitive Radio Base Station (CRBS). The CRBS allocate available channel resources to the SUs based on their QoE expectations and maintain a priority service queue. The modified ON/OFF models and Markov models of PCs and service queue models of SUs are jointly investigated for this channel allocation scheme.

In the paper "Multicarrier Authentication at the Physical Layer" [10], by constraining the allocation of power between message and authentication tag, the authentication can be made simultaneously stealthy and robust. Rather than concentrating the energy in a few high powered few carriers, it is better to use many low powered carriers to improve stealth and robustness. The main benefit of multi-carrier authentication system is improved stealth and robustness with no increase in power.

The proposed Selfish attacks and detection [11] technique, with multi channel resources by cooperative neighboring cognitive radio nodes is called COOPON (Cooperative neighboring cognitive Radio nodes).
The three types of Selfish attacks are:
Type 1: Signal fake Selfish attack.
Type 2: Signal fake Selfish attack in dynamic signal access.
Type 3: Channel pre occupation Selfish attack.
COOPON gives reliable selfish attack detection results by simple computing and well fitted for Cognitive radio Ad-hoc networks.

V - PROPOSED WORK

In order to counter the PUE attack, a proper authentication system should be provided. That Primary User authentication system should deliver PU activity information securely and reliably to the Secondary Users. Hence we propose a secured authentication with modulation that may be done at physical layer itself. We propose a method which allows primary users to add a cryptographic link signature to its signal to authenticate primary users. Signature is added through QAM modulation technique, which provides better performance and the malicious secondary users are not able to decode the cryptographic signature modulated with the signal. Simulations may be performed using Matlab, with communication tool box.

QAM is a method for sending two separate (and uniquely different) channels of information. The carrier is phase shifted in order to create two carriers namely the sine and cosine versions. The outputs of both modulators are algebraically summed and the result, which is a single signal, is to be transmitted, containing the In-phase (I) and Quadrature (Q) information. The set of possible combinations of amplitudes, as shown on an x-y plot, is a pattern of dots known as a *QAM constellation*. With the 16 QAM modulation scheme, 4 bits are processed to produce a single vector. The resultant constellation consists of four different amplitudes distributed in 12 different phases as shown in Fig. 7. As secured and higher data rates can be achieved using QAM, it is proposed for PU authentication.

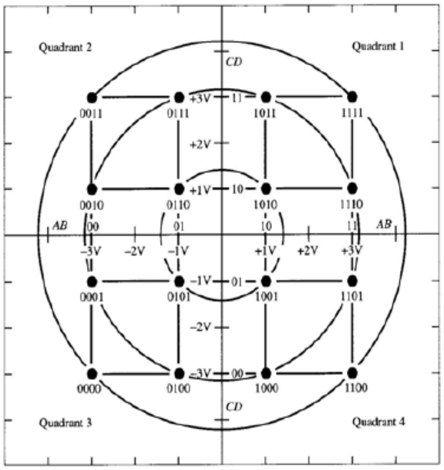


Fig.7. 16 QAM Constellations

VI - CONCLUSION

The PUE attack is the major threat in cognitive Radio Networks. It is identified and its disruptive effect on spectrum sensing is analyzed through various papers. To counter this PUE attack, an efficient primary transmitter authentication is needed. QAM provides higher data rates than QPSK. Hence instead of QPSK, future work on QAM based authentication will be done.

REFERENCES

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

[2] 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 Symp. on Security and Privacy*, pp. 286–301.

[3] B. Danev, H. Luecken, S. Capkun, and K. E. Defrawy, "Attacks on physical-layer identification," in *Proc. 2010 ACM WiSec*, pp. 89–98.

[4] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. 2011 ACM WiSec*, pp. 79–90.

[5] Swathi chandrashekarand &Loukas Lazos, "A Primary User Authentication System for Mobile Cognitive Radio Networks", Invited paper in 978-1-4244-8132-3/10/ IEEE 2010.

[6] Caidan Zhao,Liang Xie, Xueyuan Jiang, Lianfen Huang,Yan Yao," A PHY-Layer Authentication Transmitter Identification in Cognitive Radio Networks", 2010 *IEEE International Conference on Communications and Mobile Computing*, 978 -0-7695-3989-8/10

[7] Zhou Yuan,Dusit Niyato,Husheng Li,Ju Bin Song,and Zhu Han, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," *IEEE J. Sel. Areas Communications*, vol. 30, no.10, November 2012.

[8] Paul L,Yu,John S. Baras,Brain M. Sadler, " Physical-Layer Authentication", *IEEE Transactions on Information Forensics and Security*, Vol.3, No.1, March 2008

[9] Tigang Jiang,Honggang Wang and Athanasios V. Vasilakos,"QoE Driven Channel Allocation Schemes for Multimedia Transmission of Priority – Based Secondary Users over Cognitive Radio Networks", *IEEE Journal Selected Areas Communication*, vol. 30, no7, August 2012.

[10] Paul L. Yu and John S. Baras & Brian M. Sadler ,"Multicarrier Authentication at the Physical Layer", *IEEE - 978-1-4244-2100-8/08/2008*

[11] Minho Jo,Longzhe Han,Dohoon Kim and Hoh Peter In," Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks", *IEEE Network May/June 2013*, 0890-8044/13/

[12] I. A. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks:A survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

[13] B. Wild and K. Ramachandran, "Detecting primary receivers for cognitive radio applications," in *Proc. 1st IEEE Int. Symp. DySPAN*, Baltimore, MD, Nov. 2005, pp. 124–130.

BIOGRAPHY

Mrs.T.Lakshmibai is a Research scholar at SCSVMV University, Kancheepuram, Tamilnadu, India and is currently working as Assistant Professor in the EIE Dept at SCSVMV University, Kancheepuram, Tamilnadu, India, facilitating the ME, MCA & BE students academically and in their Research Work as well. She has attended various Seminars, Conferences and workshops as well. Her specialization and research work is in Wireless Communications & networking and her research interest includes Wireless sensor networks, Advanced Communication Systems, Artificial Intelligence, and Aircraft Instruments.

Mr.B.Chandrasekaran is an Assistant Professor in the Dept.of ECE, SCSVMV University, Kanchipuram. He obtained his BE in ECE from KanchiPallavan Engg College and ME Applied Electronics from C.Abdhul Hakkim College of Engg. & Tech., Vellore. His areas of interest is Wireless Communication, Image Processing and Network Security

Dr.C.Parthasarathy has been working as an Assistant professor in the Department of Information Technology in SCSVMV University, Kanchipuram since 2006. He has completed his M.C.A in Madras University, M.Tech in Sathyabama University, M.Phil (Computer Science) in Annamalai University and PhD in SCSVMV University. He started his career as Lecturer and served in various colleges. His areas of research are Network Security, Steganography, Cryptography and Soft Computing. He has attended international and National seminars, Conferences, Workshops and also presented numerous papers. Presently he is guiding PhD Scholars in the area of Wireless Communication and Network Security.