Innovative Science and Technology Publications

International Journal of Future Innovative Science and Technology,
ISSN: 2454- 194X Volume-4, Issue-2, May - 2018

RESOURCE ALLOCATION AND SCHEDULING IN COGNITIVE RADIO NETWORKS WITH ENHANCED ENCRYPTION IN 5G HETNETS

[1]T.Vignesh, M.E., [2]S.SenthamizhlSelvi, M.E.,

[1]ASSISTANT PROFESSOR, DEPT OF ECE, PEC, VANIYAMBADI.
[2]ASSISTANT PROFESSOR, DEPT OF ECE, PEC, VANIYAMBADI.

E-Mail: thiruramvigneshece@gmail.com, senthamizhlselvi116@gmail.com

May – 2018

www.istpublications.com

RESOURCE ALLOCATION AND SCHEDULING IN COGNITIVE RADIO NETWORKS WITH ENHANCED ENCRYPTION IN 5G HETNETS

[1]T.Vignesh, M.E., [2]S.SenthamizhlSelvi, M.E.,

[1]ASSISTANT PROFESSOR, DEPT OF ECE, PEC, VANIYAMBADI, Tamilnadu, India.

[2]ASSISTANT PROFESSOR, DEPT OF ECE, PEC, VANIYAMBADI, Tamilnadu, India.

E-Mail: thiruramvigneshece@gmail.com, senthamizhlselvi116@gmail.com

ABSTRACT: Cognitive radio networks have been proposed to fully utilize the radio frequency spectrum, by allowing secondary users to use the spectrum whenever primary user is not using it. To avoid interference with the primary user, secondary users should constantly monitor the usage of the spectrum. But, achieving a trustworthy monitoring is not easy. So, the Primary User Emulation (PUE) attack comes in to existence, in that a malicious secondary user makes the other secondary users into believing that the primary user is using the spectrum when it is not. To prevent this attack, primary users' spectrum usage should be authenticated. We propose a method that allows primary users to add a cryptographic link signature to its signal so the spectrum usage by primary users can be authenticated. 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 are performed using MATLAB, with communication tool box.

Keywords: *Primary User Emulation, Cryptographic Link Signature, QAM Modulation Technique, MATLAB.*

1. INTRODUCTION

1.1 Motivation and Scope

A cognitive radio is a transceiver which automatically detects available channels in wireless spectrum and accordingly changes its transmission or reception parameters so more wireless communications may run concurrently in a given spectrum band at a place. With the rapid deployment of new wireless devices and applications, the last decade has witnessed a growing demand for wireless radio spectrum. However, the fixed spectrum assignment policy becomes a bottleneck for more efficient spectrum utilization, under which a great portion of the licensed spectrum is severely under-utilized [1]. The inefficient usage of the limited spectrum resources urges the spectrum regulatory bodies to review their policy and start to seek for innovative communication technology that can exploit the wireless spectrum in a more intelligent and flexible way.

The concept of cognitive radio is proposed to address the issue of spectrum efficiency and has been receiving an increasing attention in recent years, since it equips wireless users the capability to optimally adapt their operating parameters according to the interactions with the surrounding radio environment. There have been many significant developments in the past few years on cognitive radios. Regulatory bodies in the world (including the Federal Communications Commission in the United States and United Kingdom) found that most radio frequency spectrum was inefficiently utilized. Cellular networks bands are overloaded in most parts of the world, but other frequency bands (such as military, amateur radio and paging frequencies) are insufficiently utilized [2].

Independent studies performed in some countries confirmed that observation, and concluded that spectrum utilization depends on time and place. Moreover, fixed spectrum allocation prevents rarely used frequencies (those assigned to specific services) from being used, even when any unlicensed users would not cause noticeable interference to the assigned service. Therefore, regulatory bodies in the world have been considering allowing unlicensed users in licensed bands if they would not cause any interference to licensed users

1.2 Cognitive radio network categories:

1.2.1 Depending on transmission and reception parameters, there are two main types of cognitive radio:

Full Cognitive Radio (Mitola radio), in which every possible parameter observable by a wireless node (or network) is considered.

Spectrum-Sensing Cognitive Radio, in which only the radio-frequency spectrum is considered.

1.2.2 Other types are dependent on parts of the spectrum available for cognitive radio:

- **Licensed-Band Cognitive Radio**, capable of using bands assigned to licensed users (except for unlicensed bands, such as the U-NII band or the ISM band. The IEEE 802.22 working group is developing a standard for wireless regional area network (WRAN), which will operate on unused television channels.
- **Unlicensed-Band Cognitive Radio**, which can only utilize unlicensed parts of the radio frequency (RF) spectrum. One such system is described in the IEEE 802.15 Task Group 2 specifications, which focus on the coexistence of IEEE 802.11 and Bluetooth.
- **Spectrum mobility**: Process by which a cognitive-radio user changes its frequency of operation. Cognitive-radio networks aim to use the spectrum in a dynamic manner by allowing radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during transitions to better spectrum.
- **Spectrum sharing**: Provides a fair spectrum-scheduling method; a major challenge to open-spectrum usage. It may be regarded as similar to generic media access control (MAC) problems in existing systems.

1.3 Architecture of cognitive radio network:

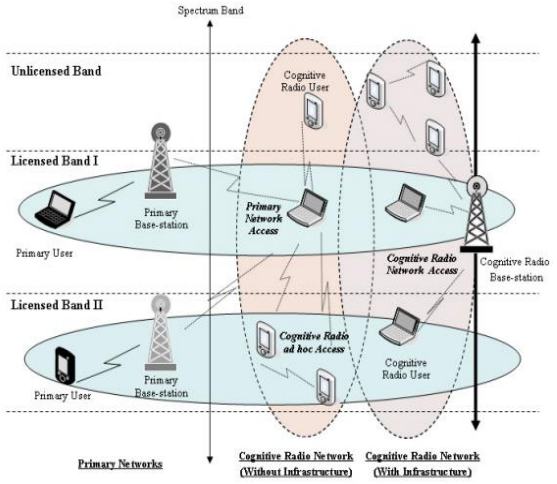

Fig 1.1: Architecture of cognitive radio network

1.4 Need for Authentication:

SERIOUS security threat to a cognitive radio (CR) network is the so-called Primary User Emulation (PUE) attack. Under PUE attack, an adversary emulates the primary transmitter, and thus effectively shutting off potential opportunity for secondary users to access the spectrum. In the presence of PUE attack, spectrum sensing mechanisms based on either energy or feature detection is incapable of offering truthful results. Thus, an effective primary transmitter authentication method is needed. We proposed an authentication scheme that integrates cryptographic and wireless link signatures [3].

1.5 Problem in existing technique:

At the heart of this scheme is a "helper node", which is in close proximity to the primary transmitter. The helper node is assumed to share similar location-based channel impulse response (temporal link signature) to that of the primary transmitter. A secondary user first authenticates the helper node through its cryptographic signature. Then the secondary user is able to authenticate a primary user based on the temporal link signature that it receives from the helper node. A strong assumption of this scheme is that no attacker is allowed to be in close proximity to the primary transmitter. Another concern of this scheme is potential single point of failure at the helper node.

1.6 Cryptographic signature:

It is an interesting authentication scheme that eliminates the need of a helper node. A neat idea in their scheme is to have the primary transmitter embed cryptographic authentication tag at the physical layer through either modulation or channel coding. This Information embedding process is equivalent to slightly perturbing the original signal purposely in a systematic manner. A secondary user will be able to extract the embedded authentication tags and perform primary transmitter authentication, while a primary receiver is expected to decode the slightly perturbed signal by treating the embedded additional information as noise [4].

2. PROBLEMS IN COGNITIVE RADIO NETWORK:

2.1 PU emulation attack:

In a direct PUE attack, the goal of the adversary is to impersonate the features of a PU signal on the idle portion of the spectrum. This can be achieved by mimicking features of PU transmissions

such as power, modulation type, synchronization sequences etc., or by recording and replaying PU transmissions.

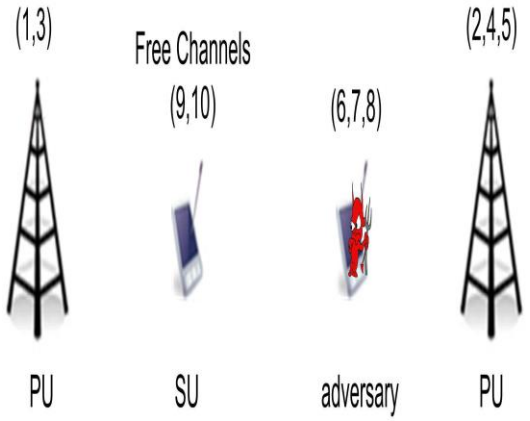

Fig 3.1 PU Emulation Attack

2.2 Problem and Main Contributions:

We address the problem of preventing PUE attacks in mobile cognitive radio networks (CRNs). We propose a PU authentication system that securely and reliably delivers PU activity information to SUs. Our system does not require any modifications to the legacy system, as mandated by the FCC. Provision of robust sensing information is facilitated by the deployment of a set of "helper" nodes. These helper nodes are responsible for authenticating the PUs and providing channel status information to the CRs. We suggest a two-way authentication system, where, the helper nodes authenticate PU activity and transmit channel availability information to the SUs[5].

The helper nodes authenticate the PU using a link signature which is a channel property between two nodes. The 17 SUs authenticate the helper nodes by verifying their cryptographic signatures. Helpers are deployed within the area of the PU network, independent of the location of the PUs, and can be relatively cheap low-power devices. Moreover, the location of the PUs need not be known. We also make use of a reputation-based system to detect compromised helpers that provide erroneous spectrum information.

2.3 Helper node problem:

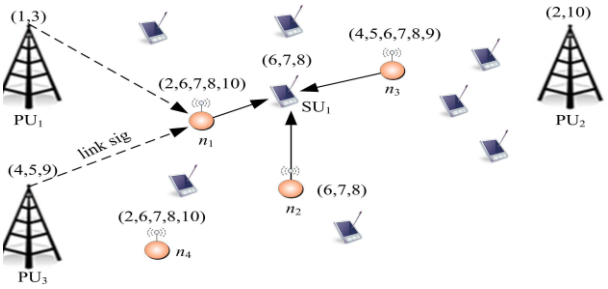

Fig 2.2 Helper node problem

We propose a PU authentication system that securely and reliably delivers PU activity information to SUs. Our system does not require any modifications to the legacy system, as mandated by the FCC. Provision of robust sensing information is facilitated by the deployment of a set of "helper" nodes. These helper nodes are responsible for authenticating the PUs and providing channel status information to the CRs. We suggest a two-way authentication system, where, the helper nodes authenticate PU activity and transmit channel availability information to the SUs. The helper nodes authenticate the PU using a link signature which is a channel property between two nodes. The SUs authenticate the helper nodes by verifying their cryptographic signatures. Helpers are deployed within the area of the PU network, independent of the location of the PUs, and can be relatively cheap low-power devices. Moreover, the location of the PUs need not be known. We also make use of a reputation-based system to detect compromised helpers that provide erroneous spectrum information.

2.4 Existing QPSK based System:

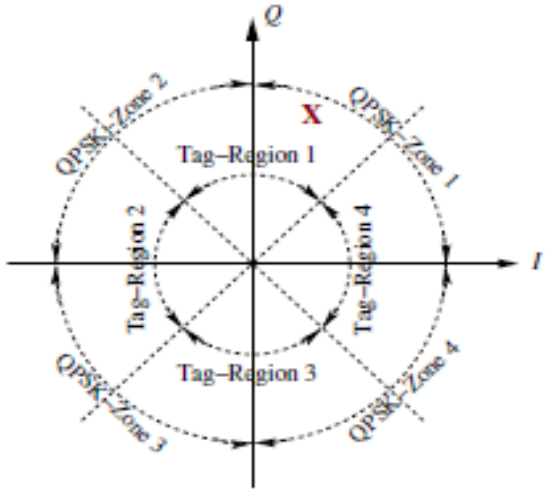

Fig 2.3 QPSK based tag generation

We focus on physical layer modulation based on QPSK and investigate how to embed authentication tag bits without significant reduction in the coverage area for the primary receivers. That is, we will find the upper bound for the phase shift required to embed authentication tag bits in QPSK modulation so as to maintain a similar size of effective coverage area for primary receivers. Based on this upper bound, we find that the effective coverage area for the secondary receivers will be significantly reduced, rendering a large percentage of secondary users unable to perform authentication function, which violates the goal of ECS-PL scheme [6].

2.5 Quadrature Amplitude Modulation (QAM)

QAM is a method for sending two separate (and uniquely different) channels of information. The carrier is shifted to create two carriers namely the sine and cosine versions. The outputs of both modulators are algebraically summed and the result of which is a single signal 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*. Consider the 16 QAM modulation scheme. With this modulator, 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. 4.1

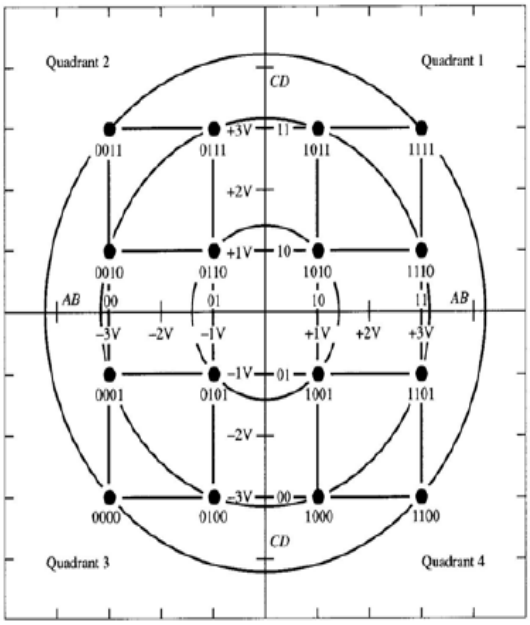

Fig. 4.6 : 16 QAM Constellation

2.6 Embedding Authentication Tags into Modulated Signals.

The basic idea of embedding cryptographic information in a modulated signal is to perturb the pre-defined QPSK phases toward the horizontal *I*-axis or the vertical *Q*-axis by an "additional" small phase θ depending on the underlying tag bit (0 or 1). Specifically, in Fig.4.1(b), for any of the four QPSK signals, if we want to embed a tag bit of 1 into the signal, we will shift an additional phase of θ toward the vertical *Q*-axis. Likewise, if we want to embed a tag bit of 0 into the signal, we will shift an additional phase of θ toward the horizontal *I*-axis. For decoding at the secondary receiver, we divide the 2π phase into four Tag-Regions, which is a $\pi/4$ counterclockwise phase shift of the four QPSK-Zones. Depending on which Tag-Region the received signal falls into, a secondary receiver will determine the corresponding tag bit. Note that after such phase perturbation, a transmitted signal will carry two pieces of information: the user data stream (a two-bit pair) and authentication tag information (one bit).

2.7 Recovering Signals and Authentication Tags at Primary and Secondary Receivers.

For the modulated signal, additional noise will be added to the signal at a receiver. Depending on which QPSK-Zone the received signal falls into, a primary receiver will determine the corresponding user data (two-bit symbol). At the same time, depending on which Tag-Region the same received signal falls into, a secondary receiver will determine the corresponding tag information (one bit). As an example, suppose a user data of 11 is being transmitted and a tag bit of 1 is to be embedded in the signal. Then the received signal is

$$\bar{S}(t,\theta) = \sqrt{\frac{2E_s}{T_s}}\cos(2\pi f_c t + \frac{\pi}{4} + \theta) + W(t),$$

where $W(t)$ is white Gaussian noise with zero mean and power spectral density $N0/2$. Referring to Fig. 1(c), suppose the received signal falls at "X". Since this point is in QPSK Zone 1, a primary receiver can determine the received user data being 11. At the same time, a secondary receiver can determine that the tag bit is 1 since the point is in Tag-Region 1. Clearly, θ is a critical parameter.

3. OUTPUTS

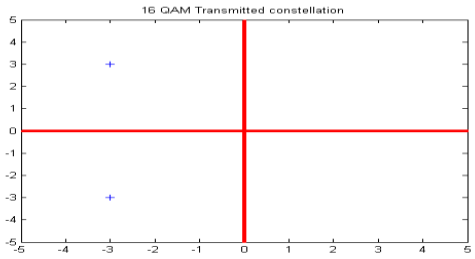

FIG1: Transmitted constellation

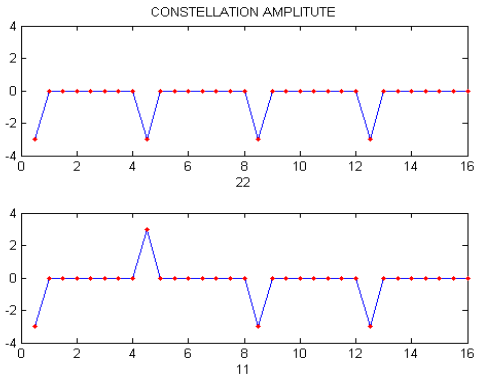

FIG2 : Constellation Amplitude (Real and imaginary)

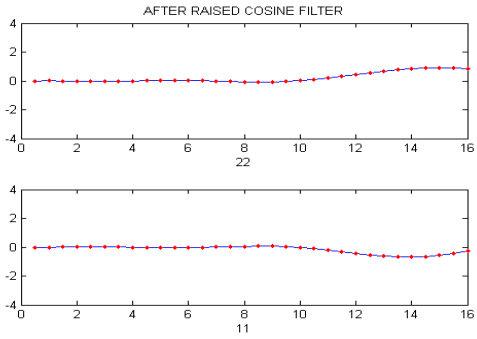

Figure 3 : After Raised cosine filter

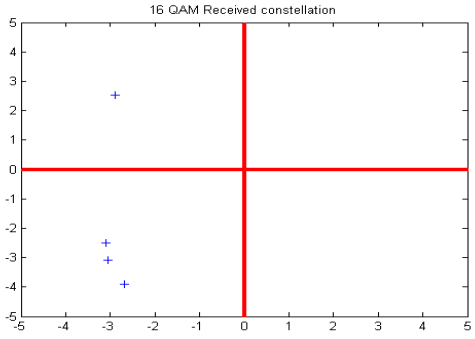

Figure 4 : Received constellation

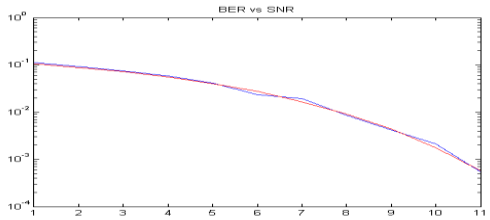

Figure 5: BER Vs SNR

4. CONCLUSION:

In this project, work has been presented which provides authentication tag for the primary user to authenticate the secondary users through QPSK modulation technique. This is very secure compare to other modulation technique. QPSK can encode two bits per symbol, with Gray coding to minimize the BER. Analysis shows that this may be used either to double the data rate compared to a BPSK system while maintaining the bandwidth of the signal or to maintain the data-rate of BPSK but halve the bandwidth needed. QPSK can be used either to double the data rate compared with BPSK system while maintaining the same bandwidth of the signal or to maintain the data rate of the BPSK but halving the bandwidth needed. But QAM provides higher data rates than QPSK. Hence instead of QPSK, QAM based authentication will be made for proposed work and has to be analyzed in second phase.

REFERENCES

[1] R. Chen, J. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE J. Sel. Areas Commun., 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 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] V. K. Garg, "Wireless Communications and Networking", Elsevier/Morgan Kaufmann Publishers, 2007.

[6] S. Lin and D. J. Costello, "Error Control Coding", 2nd edition. Pearson Prentice Hall, 2004.