International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

IMPROVED COOPERATIVE SPECTRUM USAGE INCOGNITIVE RADIO NETWORKS THROUGH MODULATION

B.Thenral[1], D.Santhosh kumari [2], R.Sarjila[3], J. Siva Guru[4]

[1234]*Assistant Professor, Dept of ECE, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India*

Abstract - The major task in cognitive radio network is to consume the spectrum effectively. Authentication process in CR network, always consumes a portion of spectrum. Hence we find a new method to mitigate this problem of spectrum wastage. We propose a new cooperative spectrum sensing for cognitive radio (CR) systems that is designed to detect low-power primary users (PUs). In previous works, all cognitive terminals (CTs) are within the no-talk zone of Primary user, which is that the province that a CT should not use the band of PU when it lies within the province. However, when the PU transmitted at low capacity, only some cognitive terminals will lies within the no-talk zone. It is therefore cleared that low-power PUs cannot be protected sufficiently. When standard sensing system are used. To solve this problem, we propose a new system in which CTs perform sensing in a number of different stages. Through simulations and performance analysis, we show that our proposed system can detect low-power PUs in which it has high accuracy, results in the protection of PUs

Key words: Spectrum usage, cognitive radio, modulation.

1. INTRODUCTION

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 are incapable of offering truthful results Thus, an effective primary transmitter authentication method is needed.. Proposed an authentication scheme that integrates cryptographic and wireless link signatures. At the heart of this scheme is a "helper node", which is in close proximity to the primary transmitter. The helper node is assumed 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. Very recently, proposed 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. For the ease of exposition, as ECS-PL (for Embedded Cryptographic Signature at the Physical Layer). At first glance, ECS-PL is appealing in a number of ways. First, ECS-PL is purely based on cryptographic signature, which is considered most effective in identifying PUE attack. Second, ECS-PL operates at the physical layer, and makes no requirement on upper layer compatibility between primary transmitters and secondary users for authentication. Such physical layer approach can support diverse population of secondary users under different upper layer protocols, as long as they understand physical layer signals. Third, it only requires a small modification of signal at the primary transmitter (i.e., TV tower). It does not require setting up any additional infrastructure such as the helper node in . As a result, it eliminates any pitfalls associated with a helper node. Finally, it is transparent to primary receivers, in the sense that no hardware/software modification is needed at primary receivers. Existing primary receivers are still able to decode their received signals as the embedded tag information is treated as noise .A performance analysis of ECS-PL focusing on user data error rate (for primary receivers) and authentication tag error rate (for secondary receivers) was we investigate ECS-PL from a different perspective. We study the effective coverage areas for the primary receivers and secondary users under ECS-PL. Specifically; 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 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. Surprisingly, our finding is independent of some important system parameters such as primary transmitter power, bit rate, antenna heights and gains, and noise spectral density.

1.1 MOTIVATIONS

The aim of the paper is to eliminate the spectrum wastage. Hence a new cooperative spectrum sensing system for cognitive radio (CR) is designed. This system can share the spectrum from primary user to secondary user

1.2 EXISTING SYSTEM

Cognitive radio networks with multi user OFDM has been designed tested.Rayleigh fading channel has been considered .Average number of bits per symbol is estimated with respect to number of RT users and with respect to number of sub channels. QPSK based signature addition is done. Based on the key whether 0 or 1, the QPSK angle is modified as shown below Encryption done with four angles So time consumption is more, because four angles are involved. The parameters are increased in the existing system primary transmitter power, signal bit rate Antenna heights and gains and noise spectral density.

1.3 PROPOSED SYSTEM

In proposed system Cognitive radio networks with multi user OFDM along with QPSK modulation has been designed and tested along with BCH codes. Moreover, modulation scheme itself is used for encryption, in order to avoid additional bandwidth Instead of embedding in four regions; we embed the signature key only at one sequence so we avoid some additional bandwidth in which we can share that bandwidth to secondary user. Hence a authentication between primary user and secondary is checked and average coverage area is calculated between primary and secondary user

3 COVERAGE DISTANCE

i) Effective Coverage Area for Primary Receivers before ECS-PL

We first calculate the effective coverage area of the primary transmitter before ECS-PL scheme is employed. Denote this area as *Ap* and its radius (transmission range) as *Rp*. Denote *Ps* as the symbol error rate at primary receiver's erfc*EbN*0 where is the complimentary error function, *Eb/N*0 is enegy per bit to noise power spectral density ratio at a receiver. So once we have a target *Ps* for a given *N*0, we can obtain energy per bit *Eb*. Once we have *Eb*, we can calculate the received signal power as *pr* = *EbBr* where *Br* is the bit rate. With *pr* and we can obtain *d*, which is also *Rp*.

(ii) Effective Coverage Area for Primary Receivers after ECS-PL after ECS-PL is employed, signal symbol error rate *Ps*_ 12erfc*EbN*0 (cos θ − sin θ)+12erfc*EbN*0(cosθ+sinθ) where θ is the phase shifting angle for embedding authentication tags. By the same token in Procedure 1, we can Computing *A*ECS-PL *pt*, *ht*, *Gt*, *hr*, *Gr*, *Ps*, *L*0, *N*0, *Br*, θ, *P* tag *e* , BCH(*n*tag,*k*tag, *t*tag) and *L* compute the effective transmission range (denoted as *R*ECS-PL) as well as the coverage area (denoted as *A*ECS-PL*p*) for primary Receivers after ECS-PL is employed.

(iii) Effective Coverage Area for Secondary Receivers aftervECS-PL After ECS-PL is employed, secondary receivers will receive the same signal as primary users but are only interested in decoding the tag information for authentication The tag bit error rate, denoted as *Pt*, *Pt* _ 12erf Even more important than *Pt* is the tag error rate, denoted as *P* tag*e* , which is defined as the probability of having one or more bits in error in the *L*-bit authentication tag and should be kept extremely low, e.g., below . Such stringent requirement is due to the fact that an authentication tag (with *L* bits) is a cryptographic hash value, which cannot tolerate even a single bit error. To keep *P* tag*e* low, error correcting codes (ECC) can be used. First, a *L*-bit authentication tag is broken up into a number of *k* tag-bit segments. Under ECC, each *k*tag-bit segment is encoded into *n* tag-bit codeword, which can correct up to *t*tag-bit errors. Denote *P* tag *cw* as the probability that the received *n*tag-bit codeword is in error. Then *P*tag*cw* is upper bounded by *P*tag*t* (1 − *Pt*)*n*tag−*i*, (6)where *Pt* is the tag bit error rate in (5). With *P*tagin (6). Then, we can follow the same token a to obtain the effective transmission range (denoted as *R*ECS-PL*s*)and coverage area (denoted as *A*ECS-PL*s*) for secondary receivers.

Wideband noise comes from many natural sources, such as the thermal vibrations of atoms in conductors (referred to as thermal noise or Johnson-Nyquist noise), shot noise, black body radiation from the earth and other warm objects, and from celestial sources such as the Sun. The central limit theorem of probability theory indicates that the summation of many random processes will tend to have distribution called Gaussian or Normal.

3.1 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

3.2 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)

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

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 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. It is very clear from the results that, the BCH code, of 1023,11 performs well both for BPSK and QPSK and the performance of QPSK is better than BPSK, hence a stronger can been added without adding any additional bandwidth .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.

3.4 BLOCK DIAGRAM

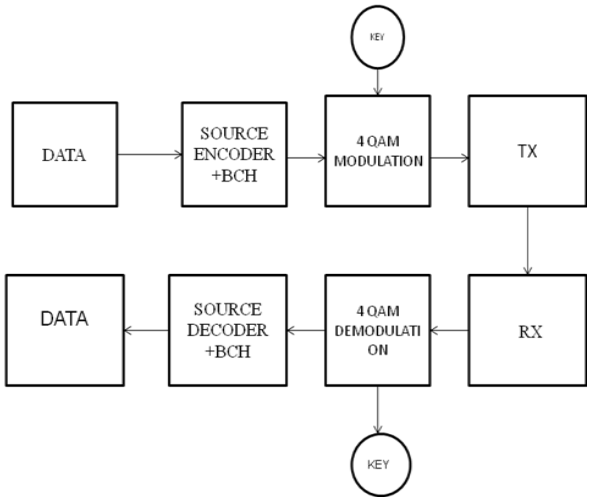

Fig.4 Block Diagram

STEP 1: Generate the key(01101001)

STEP 2: Fix the constellation angle

STEP 3: Generate the random data 11 bits in matrix dimension

STEP 4: Encoded the data with BCH encoder (all these process is in 0,1)

STEP 5: Before modulation process converts binary into integer

STEP 6: Modulation with a function Gen QAM modulation

STEP 7:Plot the transmitter constellation point(just to verify the constellation point and constellation array)

STEP 8: modulation signal passed through channel where it is added with AWGN

There are two receive In primary Receiver Demodulation is done and the data is decoded then output data is converted decimal into binary then we Compare between transmitter and primary receiver in secondary receiver We Retrieved the given key If both key is matched then Secondary user will be authenticates

3.5 COMPARISION TABLE

BCH CODES	CONSTELLATION ANGLE	QPSK
127,50	5	0.744
	7	0.723
	10	0.644
511,10	5	0.586
	7	0.482
	10	0.466
1023,11	5	0.471
	7	0.375
	10	0.324

Fig.2 Comparison of BCH Codes, Constellation Angle

4 CONCLUSION

In this paper, The Output which provides authentication tag for the primary user to authenticate the secondary users through QPSK modulation technique which is obtained by MATLAB. This is very secure compare to other modulation technique. It is very clear from the Output that the BCH code, of 1023,11 performs well both for BPSK and QPSK and the performance of QPSK is better than BPSK, hence a stronger data can been added without adding any additional bandwidth.

5 References

[1] Woongsup Lee, Dong-Ho Cho "Improved Cooperative Spectrum Sensing in Multiple Stages for Low-Power Primary Users" IEEE wireless communications letters, vol. 2, no. 3, june 2013

[2] Joseph mitola 111 and gerald q. maguire, jr "Draft standard for wireless regional area networks," IEEE 802.22 draft standard, "IEEE P802.22TM/D0.1 IEEE 802.22 doc. no. 22-06-0068-00-0000, May 2006

[3]Sahai, N. Hoven, S. M. Mishra, and R. Tandra, "Fundamental tradeoffs in robust spectrum sensing for opportunistic frequency reuse,"Tech. Rep., 2006.

[4]W. Lee and D.H. Cho, "Enhanced spectrum sensing scheme in cognitive radio systems with MIMO antennae," IEEE Trans. Veh Technol., vol. 60,no. 3, pp. 1072–1085, Mar. 2011.

[5]V. Fodor, I. Pescosolido, and L. Pescosolido, "Detecting low-power primary signals via distributed sensing to support opportunistic spectrum access," in Proc. 2009 IEEE ICC, pp. 1–6

[6]S. Chunhua, Z. Wei, and K. B. Letaief, "Cooperative spectrum sensing for cognitive radios under bandwidth constraints," in Proc. 2007 IEEEWCNC, pp. 1–5.

[7]Simon Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications" IEEE journal on selected areas in communications, vol. 23, no. 2, February 2005 2,

BIOGRAPHIES

B. Thenral has completed her graduation in B.ECE in the year 2005 at GGR College of Engineering affiliated to Anna University, Chennai, India and completed her post graduation in M.Tech Applied Electronics in the year 2008 at M.G.R University, Chennai, India. She has been working as Assistant professor at Ganadipathy Tulsi's Jain Engineering College, Vellore, India for the past 11 years. She is working towards her research in the field of Mobile Ad-Hoc Network. Her area of specialization includes Microprocessors, RF & Microwave Engineering and Ad-Hoc Networks.