Biomedical Research 2017; 28 (6): 2830-2835 *ISSN 0970-938X*
www.biomedres.info

Helper node based effective spectrum sensing and defense against physical layer attack in cognitive radio network.

Avila Jayapalan*, Thenmozhi Karuppasamy

Department of Electronics and Communication Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract

This work focusses on a new, efficient energy detection based spectrum sensing and in addition mitigating the threats of the physical layer of cognitive radio. The Fast Fourier Transform (FFT) of the energy detection method is concatenated with Gould transform. Concatenated approach along with proper choice of windows and its size resulted in improved probability of detection and improvement in signal to noise ratio. Many new classes of security, threats and challenges may be introduced in Cognitive Radio (CR) where attackers could destroy the fundamental function of cognitive radio network and may cause interference to primary users which is not desirable or may deny the licensed spectrum of Primary users (PU) to other secondary users by surpassing PUs in cognitive radio. This is called the Primary User Emulation (PUE) attack. This paper concentrates on dipping the primary user emulation attack by means of an authentication technique. This is achieved by embedding an authentication tag in the error control code, specifically turbo code. This tag is based on chaotic Pseudo Noise (PN) sequence algorithm and Katayapadi algorithm and the same has been implanted in Field Programmable Gate Array (FPGA)

Keywords: Cognitive radio, Energy detection, Gould transform, Primary user emulation attack, Authentication tag, Turbo codes, Field programmable gate array.

Accepted on November 21, 2016

Introduction

Our radio resource is very limited and most of them are not utilized in an efficient manner. This underutilization problem could be overruled with the aid of cognitive radio. Cognitive radio [1,2] become an encouraging technology to determine the unused spectrum in the frequency band and allows the secondary users to access the free spectrum without interfering with the licensed user (primary user). The unused part of free spectrum or spectrum holes can be found out by a technique called spectrum sensing [3]. Some of the spectrum sensing techniques are energy detection [4], cyclostationary [5,6] and matched filter method [7]. Energy detection gains popularity because of simple nature.

Any intruder [8] might transmit a signal with features to imitate the PU's signal or a signal having higher power such that it is above the fixed threshold to confuse the receiver. As a result of this, secondary users will count the attacker's signal to a primary user's and thus not use the corresponding band. In PUE (Primary User Emulation) attack [9,10], it is possible that the attacker can imitate a PU and thus make a secondary user misinterpret that the spectrum is engaged by a PU.

Having the above mentioned problem in mind, it is essential to maintain a secure method that distinguishes the PU's signal from that of the attacker. According to FCC, "The incumbent system or the primary user should not be modified to lodge the occasional usage of the channel by the secondary users" Hence, using a helper node this secure communication is achieved. This helper node plays a vital role since the primary user cannot be changed owing to the FCC rules but a helper node can be modified [11,12].

Helper node

The helper node located very near to the PU [13] receives the signal from the primary user and checks the presence or absence of primary user. If the primary user is absent the helping node transmits a signal to the cognitive radio with the authentication tag. The helper node is assumed to be in the close proximity of the primary user and it is a highly protected system. The helper node does not face any hidden node problem. The nature of the tag and other details of the tag are already known to the cognitive user. In this work, in the parity bit of the turbo code, the authentication tag [14,15] is embedded.

The main purpose of adding tags of authentication in an ECC module is exploit the feature of error correction capacity of the code. In order to implant a tag, we deliberately corrupt the symbols at chosen spots in a code word from the transmitter. On the condition that the number of errors in that sequence (Errors that were embedded and the errors that occurred naturally) is than a certain 't', the error correction code module

[16] at the receiver side will correct all code words. Thus, non-CR receivers will interpret this as usual as the tags are transparent to such kind of receivers. The simulation results are plotted out using Modelsim tool and the hardware counterpart of that is carried out using Cyclone II FPGA. This tag is derived from Chaotic PN sequence code and Katayapadi Unicode.

Related Works

Spectrum sensing is one of the vital tasks of cognitive radio. In this work instead of cognitive radio carrying out the spectrum sensing, relies on helper node. Hence the sensing of the primary user is done by the helper node. To enhance the performance of energy detection based spectrum sensing, FFT of energy detection method is concatenated with Gould transform.

Gould transform

Unlike other transforms (eg. FFT) which converts the signal from one domain to other domain, Gould transform is a standard one which does the process in the same domain. Another unique property of Gould transform is that the elements of forward and inverse transform matrices are zero below the constant main diagonal and sub-diagonals.

The forward Gould transform is given by,

$$A_n = \sum_{n=0}^{N-1} p_{g,nk} y_k where\ n = 0, 1, 2 \ldots . N-1$$

A=Cy, where y, A represents Nx1 vectors and C represents N × N.

${}_N{}^gC$ is the general representation where N represents the size and g represents the integer value.

Algorithm

Step 1: The forward Gould transform A for y data is computed by the formula A=Cy where is the N*N Gould transform matrix. If the specified value for N is 2 the output of Gould matrix would be 2*2.

Step 2: Get the values of g and N for calculating forward Gould transform since matrix C is of form ${}_N{}^gC$

Step 3: For the values of g=1 and N=2, gould matrix C has 2 rows and 2 columns. Each element contained in the matrix is of form n*k. As given below when n=1 and k=0 matrix value is -1

$$2^1C = \begin{matrix} 1 & 0 \\ -1 & 1 \end{matrix}$$

Step 4: g_{n-k} can be computed with the following formula

$$g_{n-k} = \frac{g!}{(n-k)!(g-n+k)!}$$

Step 5: With the calculated g_{n-k}, (P_g, n_k) is calculated as

$$(P_g, n_k) = (-1)^{n+k} * (-1)^{n+k} [17, 18]$$

Tag generation

To generate the authentication tag two types of rules are used

- Chaotic Pseudo Noise (PN) sequence
- Katayapadi algorithm

Chaotic PN sequence: PN sequence codes are deterministically generated but resemble noise characteristics. Quantizing the output of logistic map yields chaotic PN sequence, where logistic map is mapping technique of degree two. The chaotic PN sequence is generated using the formula

Z(j+1)= B.z(j).(1-z(j)

Where j is the number of iterations

B is the system parameter

Z(0) is the initial condition [19]

Katapaya coding rules: Vedic mathematics facilitates in enjoying amazing applications of arithmetic operation, compound multiplication, basic number theory, quadratic and higher order equations, squaring, cubing, factorization, square roots, cube roots, co-ordinate geometry, differentiation and integration. The Katapayadi or Vedic numerical code was used by the mathematicians of that period, to denote the numbers. It is a potential tool to translate names to numbers [20].

- Whenever two or more consonants come together as a sequence, the last of it alone will be considered. A consonant without any vowel is ignored.
- Vowels that stand alone are considered to have zero value. Eg: a and ṛ
- Decimal separator system cannot be accommodated.
- If a vowel follows a consonant, it is assumed to have no value and if the vowel does not have any consonants in front of it, then it is assumed to have zero value.
- The digits are arranged from left to right.

Example: Considering the word “setuvandya”. Now, sa=7, ta=6, va=4, ya=1. The katapaya translated code is 1467 which is the decimal equivalent of it. In order to transmit a data using digital communication technique, it is necessary that it should be in the binary form. The binary code of the above mentioned decimal code is 0001|0100|0110|0111

FPGA Implementation

The ALTERA DE1 (Development and Education) board is mainly used for college laboratory use in understanding digital logic, computer organization and FPGA. Attributing to the Cyclone II 2C20 FPGA it is used for various tasks in digital logic and computer organization that are at different levels of design. Also, the DE1 board supports standard I/O interfaces along with a control panel which helps in accessing the components. The software demonstrates the advanced features of DE1 board. The control panel allows the user to control the components on the board using a USB connection from any host computer. Like the first generation 130 nm Cyclone FPGA, 90 mm Cyclone II are built with low cost and customer

defined feature set for those applications which are cost specific. These are known for their high performance and low power consumption. Since it is supported by easy to use and free web edition for Quartus II, the development kits are easily available for low costs [21,22].

Proposed Methodology

Spectrum sensing is one of the important functions of cognitive radio which is carried out to detect the availability of free spectrum. In this work energy detection based spectrum sensing method is considered by the helper node. To enhance the working performance FFT of the energy detection method is concatenated with gould transform.

Gould transform based energy detection

Figure 1 shows the block diagram of the concatenated method. The incoming signal along with noise is filtered and passed to the FFT block. The output obtained from this block is allowed to pass through Gould transform block. The concatenated output is fed to windowing function block followed by magnitude squaring device. The average energy obtained is now compared with the predefined threshold. The decision is based on the hypotheses namely

H0: Z (n)=c (n)-primary user absent

H1: Z (n)=w (n)+c (n) -primary user present

where, c (n)=noise, w (n)=transmitted signal, Z (n)=received signal

Figure 1. *FFT and gould transform based Energy detection method.*

Primary user emulation attack (PUEA)

One of the most important attacks in the physical layer of cognitive radio network is the PUEA. In the absence of PU to gain access of the spectrum of its own the malicious user imitates the PU which leads to a wrong decision about the occurrence of the PU. This attack is termed as PUEA. The occurrence of PUEA and its counter measure through authentication based scheme have been presented in Figure 2a to Figure 2d which were picturized using CISCO network tracer tool. Figure 2a shows a model wireless environment with PU, malicious user and secondary users. In the absence of PU the cognitive users in order to access the free spectrum, sense the availability of the PU. Figure 2b shows the PUEA targeted towards the cognitive user by the malicious user. Figure 2c shows the inclusion of helper node in the cognitive network. To overcome the PUEA, the cognitive usert deploys a reliable third party known as helper node. One of the responsibilities of the helper node is to sense the presence or absence of PU. Gould transform based energy detection is utilized. In the absence of PU and if the spectrum hole is available, the helper node conveys the intended information to the cognitive receiver. Figure 2d portrays the data transfer between the helper node and the cognitive user. In the absence of PU, a specific authentication tag is generated, embedded in the parity bits of the error control code and transmitted by the helper node to the cognitive receiver. The cognitive receiver on receiving the tag compares it with the database, and validates the information based on the match. Thus PUEA is mitigated with the inclusion of helper node and by transmitting the authenticated tag through the helper node.

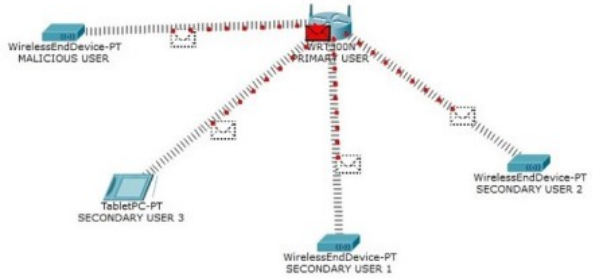

Figure 2a. *Cognitive radio network.*

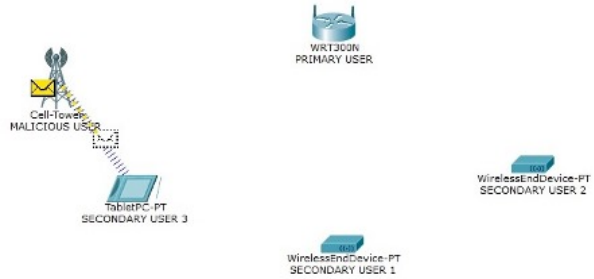

Figure 2b. *Malicious user imitating like primary user.*

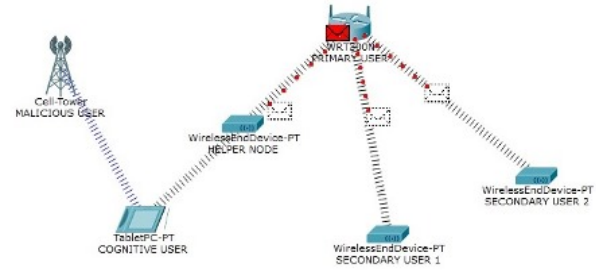

Figure 2c. *Cognitive radio network with malicious user and helper node.*

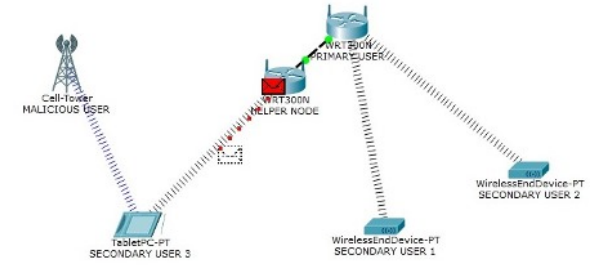

Figure 2d. *Authentication tag from helper node.*

Results and Discussion

Figure 3 shows a comparison between FFT and FFT concatenated with Gould transform. For the probability of detection of 0.9 the SNR is -20 dB in case of concatenated case whereas it -13 dB in case of FFT approach. This is helpful in detecting the primary user even in weak SNR conditions.

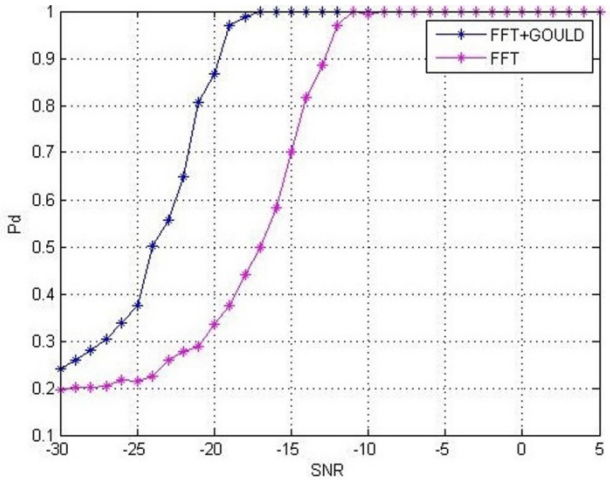

Figure 3. *Comparison between FFT and FFT+gould transform.*

Figure 4 shows the comparison between different window functions. For the probability of detection of 0.9 the SNR in case of Kaiser Window is -13 dB whereas the SNR value is -10 dB in case of hamming window. Kaiser window offers better results in weak SNR conditions because of the reduced sidelobes when compared to other function.

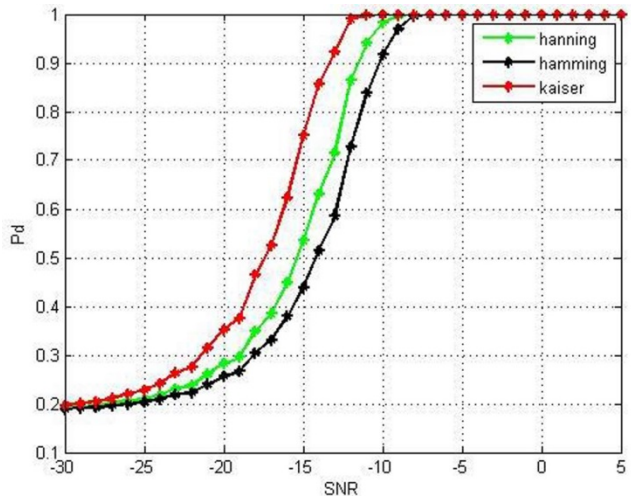

Figure 4. *Comparison between window function.*

Figure 5 shows the graph plotted between probability of detection and SNR before embedding the chaotic PN sequence and after embedding the chaotic PN sequence. The overlapping of the curves indicated that there is no significant change in the probability of detection after embedding the PN sequence. In this way authentication is achieved.

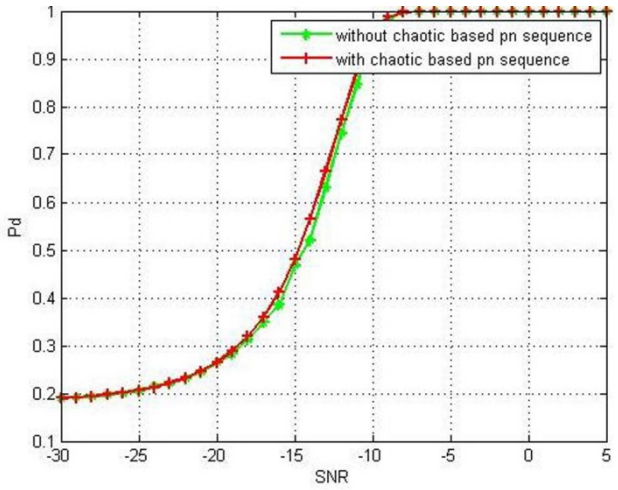

Figure 5. *Before and after embedding the chaotic PN sequence.*

Figure 6 illustrates the output of convolutional encoder. The Hardware Description Language (HDL) code for shift register based convolutional encoder was compiled and simulated using Modelsim tool. The rate of the convolutional coder is ½. The generator polynomial is (111) and (101). The message bit is set as (1011). The output of convolutional encoder is obtained by multiplying the message signal with the generator polynomial and performing XOR addition. The concatenated output is 100111 110001.

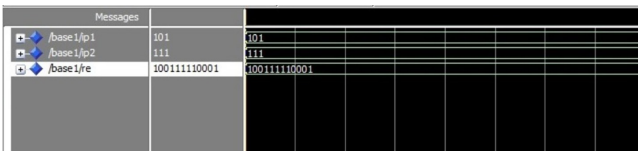

Figure 6. *Output of convolutional encoder.*

Figure 7 shows the output of turbo encoder. Turbo encoder was designed by combining two convolutional encoders separated by an interleaver. Interleaver was used in conjunction with the error correcting codes to scramble the symbols. This in turn reduces the burst errors. Interleaver can be used in series or in parallel combination with the convolutional encoder. In this work series combination has been adopted. The constraint length and rate of the convolutional encoder were fixed as K=3 and k=1/2 respectively. The generator polynomials employed were (1,1,1,) and (1,0,1). The output of first convolutional encoder is (10011111001). It is fed as input to the interleaver. Here interleaving operation has been performed through XOR operation of a known sequence. The output of interleaver is 110001001111. It is fed as input to the second convolutional coder. The concatenated output without embedding is 111101011100111001010111101101. It is XORed with the Katayapadi code and the embedded output is 011111011100111001010111101101.

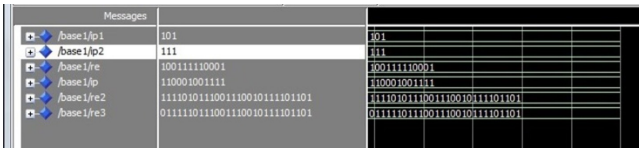

Figure 7. *Output of turbo encoder.*

Figure 8 shows the cyclone II FPGA implementation of the authentication scheme. The modeled turbo encoder was implemented on cyclone II FPGA. Cyclone II FPGAs provide low cost solution design applications which can be programmed with the bit steam generated using Quartus II Integrated Development Environment (IDE). The output is displayed with the aid of LED indicators. The red LED's indicates the output of the turbo encoder without embedding. The green LED's indicates the output of turbo encoder after embedding. Thus the error control code based authentication scheme has been implemented in cyclone II FPGA.

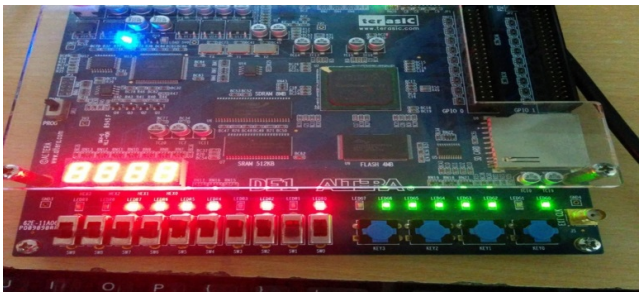

Figure 8. *Cyclone II FPGA implementation of authentication algorithm.*

Conclusion

This work deals with two aspects in cognitive radio. First one is efficient energy based spectrum sensing by concatenating FFT with Gould transform. Concatenated approach offered better SNR and probability of detection. Second the work also focused on mitigating the primary user emulation attack by the inclusion of an authentication tag in the parity bits of the turbo code. The authentication tag is generated with the aid of Katayapadi algorithm and chaotic PN sequence algorithm. To gain the advantage of reprogrammability it is implemented in FPGA.

References

1. Mitola J, Maguire GQ. Cognitive radio: making software radios more personal. IEEE Personal Communication 1999; 64: 13-18.
2. Haykin S. Cognitive radio: Brain empowered wireless communications. IEEE J Select Areas Commun 2005; 232: 201-220.
3. Kim H, Shin KG. In-band spectrum sensing in cognitive radio networks: energy detection or feature detection. 2008 Proceedings of the 14th ACM international conference on Mobile computing and networking,14-19 September, San Francisco, USA 2008.
4. Avila J, Thenmozhi K. Wavelet supersedes FFT in MB-OFDM: An effective cognitive spectrum sensing. J Artific Intell 2012; 53: 113-121.
5. Yuan Q, Tao P, Wang W, Qian R. Cyclostationarity-based spectrum sensing for wideband cognitive radio. IEEE Proceedings WRI International Conference on Communication and Mobile Computing, Yunnan 2009.
6. Prithiviraj V, Sarankumar B, Kalaiyarasan A, Praveen Chandru P, Nandakumar Singh N. Cyclostationary analysis method of spectrum sensing for cognitive radio. IEEE 2011 International conference on wireless communication, vehicular technology, Information theory and Aerospace & Electronic system technology (wirelesss VITAE), Chennai.
7. Yucek T, Arslan H. A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Commun Surveys Tutorials 2009; 111: 116-130.
8. Xie X, Wang W. Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. J Ubiquitous Syst Pervasive Networks 2014; 51: 1-8.
9. Borle KM, Chen B, Du W. A physical layer authentication scheme for countering primary user emulation attack. In: IEEE 2013 International Conference on Acoustics, Speech and Signal Processing (ICASSP), Vancouver.
10. Salem FM, Ibrahim MH, El-wahab IAA. Secure authentication scheme preventing wormhole attacks in cognitive radio networks. Asian J Comput Sci Informa Technol 2013; 24: 52-55.
11. Salem FM, Ibrahim MH, Ibrahim II. A Primary User Authentication Scheme for Secure Cognitive TV Spectrum 2012. IJCSI Int J Comput Sci Issues 2012; 94: 157-166.
12. Fragkiadakis AG, Tragos EZ, Askoxylakis IG. A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys Tutorials 2011; 151: 428-445.
13. Liu Y, Ning P, Dai H. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. IEEE Symposium on Security and Privacy (SP), Oakland 2010.
14. Alahmadi A, Abdelhakim M, Ren J, Li T. Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. Global Communications Conference (GLOBECOM), Atlanta, USA 2013.
15. Alahmadi A, Abdelhakim M, Ren J, Li T. Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Transact Informa Forensics Security 2014; 95: 772-781.
16. Tan X, Borle K, Du W, Chen B. Cryptographic link signatures for spectrum usage authentication in cognitive radio. Proceeding of the fourth ACM conference on wireless network security, Hamburg, Germany, 2011.
17. Le HM, Aburdene M. The discrete Gould transform and its applications. Proceedings of SPIE, 2006.

18. Varsaki EE, Fotopoulos V, Skodras AN. A discrete Gould transforms data hiding scheme. J Mathe Methods Appl Sci 2014; 372: 283-288.
19. Swami DS, Sarma KK. A Chaos based PN sequence generator for direct-sequence spread spectrum communication system. Int J Circuits Syst Signal Process 2014; 8: 351-360.
20. Bhat KR, Raajan NR. A new approach to language based encryption using Devanagari text. Int J Appl Eng Res 2014; 98: 925-928.
21. Abdulrahman A, Emhemed A. Implementation 7 segment display by educational board-software/hardware interfacing. Int J Eng Res Appl (IJERA) 2012; 2: 748-751.
22. Laddha NR, Thakare AP. A novel approach for displaying data on LCD directly from PC using FPGA. Int J Emerg Sci Eng (IJESE) 2013; 16: 106-111.

***Correspondence to**

Avila Jayapalan

Department of Electronic and Communication Engineering

SASTRA University

India