Middle-East Journal of Scientific Research 21 (9): 1498-1502, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.21.09.21607

Concatenated Error Control Code Based Authentication to Combat Primary User Emulation Attack

J. Avila and K. Thenmozhi

ECE, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract: The primary intention of this paper is to combat the effect of Primary User Emulation Attack which is the main security issue in physical layer of cognitive network. The authentication information is solely known and shared between only the intended secondary users and the helper node. Here this helper node is the overall coordinator for this authentication information exchange. This task is done in such a way that there is no much deviation in the bit error rate (BER) of the system.

Key words: Cognitive radio · Primary User Emulation Attack (PUEA) · Hash algorithm · Error correcting codes

INTRODUCTION

The rapid development of various communication and wireless technologies had led to ultimate spectrum insufficiency. This may cause a great spectrum extinction thereby not allowing new wireless services to be installed. To overcome this great spectrum disaster and to optimally use the underutilized bands, a new technology so called cognitive radio has been evolved. This technology scampers the software programs thereby helps cognitive user to look for spectrum holes, pick the best among them, work jointly in coordination with other users and do not disturb the owner of spectrum on arrival [1]. The members do stay connected in an ad-hoc manner and there is no guaranteed network architecture. This makes the privacy issues more intricate than in conventional wireless devices [2]. The medium of transport is free air, any adulteration of data can be done without much being noticed by the sufferer and at the worst case, the data signals are even jammed. Establishing security in these networks is a risky task because of its inimitable quality. [3]. The innate temperament of it has made it an open play ground for attackers.

There are four layers in a cognitive network out of which Physical layer is the lowermost layer and various attacks are feasible here. The main focus of this research work is on attacks in the physical layer since it is the common layer and has compatibility with all other devices. The rapid development of technology has led to a new attack so called Primary User Emulation Attack wherein the imitation of spiteful user as a primary transmitter occurs to deceive the secondary users and gain access over the white space.

Better functioning of the Cognitive network is affected to a great extent if this Primary User Emulation Attack is severe [4]. To predict the primary user arrival, energy detection and cyclostationary methods are used [5]. The first technique is based on the fact that the signals from primary users are periodic and do have regular cyclo stationarity property. The second method involves comparison of energy level of the signal with a preset threshold [6]. These methods are already bypassed owing to the rapid growth of technology. It can be done either by impersonating the primary transmitted signal or high power signal to confuse the energy detector [7].

Thus to avoid the problem of PUEA, we need a trustable method to verify the arrival of primary user. One such method is verification of licensed user by means of biased reaction signalling [8]. The other technique involves LocDef, where we use localization technique by non interactive technique [9]. We can also use Public encryption systems thereby ensuring the trustworthy communication [10]. Primary user has a closely placed helper node which plays the role of a bridge thereby enabling of the verification of the primary user's signals using cryptographic signatures and authentic link signatures [11]. There are hand off techniques meant for secret communication of sharing session keys between the client and the router [12].

Corresponding Author: J. Avila, ECE, SASTRA University, Thanjavur, Tamil Nadu, India.

In this research work a tag is added for authentication in a transparent way so as not to interfere with the primary receiver but still maintain authenticity with the cognitive user. The tag is added in the parity bits of the codeword or in the modulation scheme [13]. To reduce the errors introduced in transmission and enable better recovery of authentication tag, various error control codes can be used.

A convolutional encoder is a linear predetermined-state device with n algebraic function generators and K stage shift register. The binary input data, is shifted as b bits at a time along the registers. Decoding can be done by sequential decoding, maximum likelihood or feedback decoding [14].

In case of turbo codes, two RSC elementary codes are in a parallel organization. Maximum A Posteriori algorithm is used for decoding it in iterative process [15]. These codes were first developed in 1993 which were used for higher performance matching that of channel capacity at a specific noise level. Practical areas of application include deep sea communication, 3rd generation mobile networks and satellite communication applications. This enables a good reliability of transmission in bandwidth constrained applications.

In case of alamouti codes, the multiple data copies are being transmitted by multiple antennas and multiple copies thus received are being examined to get accurate results at the receiver end. The various factors which normally affect fact data transmission in a wireless environment include refraction, scattering, thermal noise and reflection etc. Thus out of various copies received, each one will be better in its own way. Thus out of multiple copies, the best features are extracted and decision is made.

Here the data is block encoded and spread via these antennas at varying time slots and thus received by one or more antennas at the receiving end and this technique forms diversity reception.

In a highly noisy environments single error control codes do not have high coding gain. In order to improve this concatenated codes are preferred [16]. Hence to cope up with the FCC regulations, we proposed a method in which the authentication tag is embedded onto the data signal by the helper node after encoding and the comparative study of which concatenated codes serve the best to reduce the bit error rate has been discussed.

MATERIALS AND METHODS

Hash Algorithm: Message is Padded in such a way that the length of message matches to 896 modulo 1024. In certain cases, the length may match yet the padding becomes additional. In order to make the desire length, a binary bit 1 is added followed by as many zeros as required to make the desired length. Depending upon the actual message size, the number of bits padded varies from 1 to 1024 itself. Thus, the message after padding is an unsigned integer of 128 bits and output of earlier two steps is a 1024 bit integer in order to calculate the length of message. Eight registers each of capacity to hold 64 bits (p, q, r, s, t, u, v, w) are needed to grasp the 512 bit results momentarily. This 512 bit output is carried over as an input to the consecutive stages. For the first stage, the previously stored transitional hash output is taken. On processing the padded message of 1024 bits, we get 64 bit as input per round. So to maintain the security and avoid repetitions, we do use a constant to point to the round number out of 80. After completion of 80 rounds, the final stage result is fed back to the first block until the message gets over. Thus (Oi-1) is needed to generate Oil where I is the stage number.

Here, it is assumed that the primary transmitter and the helper node share almost the same geological location and the helper node has a secret communication with the secondary users there. The primary transmitter on arrival generally transmits a data signal to its intended primary receiver. Since the primary transmitter has the highest priority and in no way it should be interfered we use the helper node to embed this security tag. The primary transmitter encodes the data sequence, modulates and transmits the signal. The data sequence after encoding is modulated and being transmitted by the primary transmitter. The helper node here repeats the signal and the hashed output is being embedded by it. Here the embedding is done in such a way that the tag to data ratio is comparatively low.

Step 1: The hash algorithm and key for it is being exchanged securely between the helper node and the cognitive users involved in the process.

Step 2: The message signal is being encoded by the primary transmitter user either of the encoding schemes like convolutional code, turbo code or any of the preferred concatenated codes.

Step 3: In case of convolutional encoder of rate ½, the number of message bits is being doubled.

Step 4: The number of encoded bits are taken to be 1, 50,000 in number.

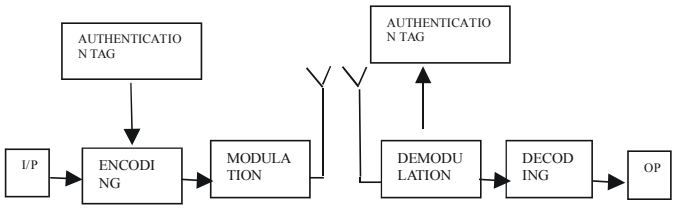

Fig. 1: Block diagram of the model

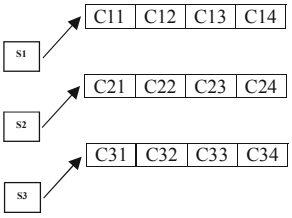

Fig. 2: Embedding of tag into codeword

Step 5: These bits are divided into blocks of 300 bits each and form the symbols C11, C12, C13 etc.

Step 6: The 512 bit hash output is divided into 16 blocks each of 32 bit in size and they form the symbols S1, S2, S3 etc.

Step 7: The first symbol in each codeword, the first 32 bits is replaced with these 32 bits of hash.

Step 8: The same method is repeated till the end of data signal.

This method can be used for N bit codeword with M bit hash based on the requirement. The tag thus obtained is substituted in the place of first p bits of the total N code words obtained. We do obey the regulations as per FCC since this tag embedding task is solely performed by the helper node and the number of bits embedded is too low without much affecting the primary receiver. This tag is treated as noise by the primary receiver and discarded. At the receiver end the authentication tag is retrieved and checked for authenticity. This tag verification is being done by the Cognitive Radio user upon reception since we did assume that the key for hash had been exchanged privately earlier. If verification is successful, the task is suspended and secondary user looks for any new white space.

RESULTS AND DISCUSSION

Figure 3 shows the system with and without embedding. Here turbo code is used as error control code. BPSK modulation scheme is used. Form the figure it is evident there is no significant variation in the BER of the system before and after embedding.BPSK modulation scheme is less error prone when compared with other modulation schemes but it supports less data rate.

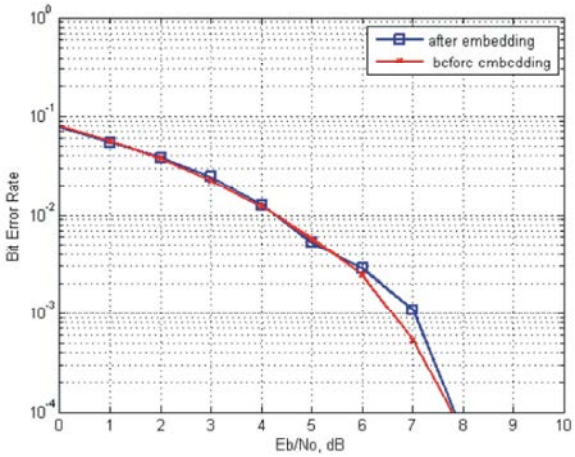

Fig. 3: System beforeand after embedding with Turbo code

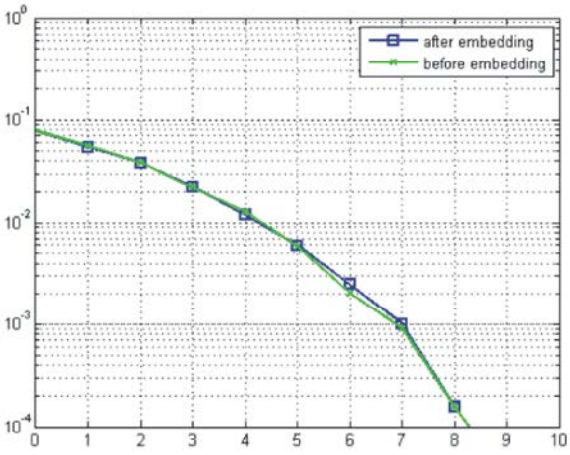

Fig. 4: System beforeand after embedding with Turbo code+QPSK modulation

Figure 4 shows the system with and without embedding. Here turbo code is used as error control code. QPSK modulation scheme is used. From the figure it is evident there is no variation in the BER of the system before and after embedding. QPSK modulation scheme is less error prone when compared with QAM and supports high data rate than BPSK.

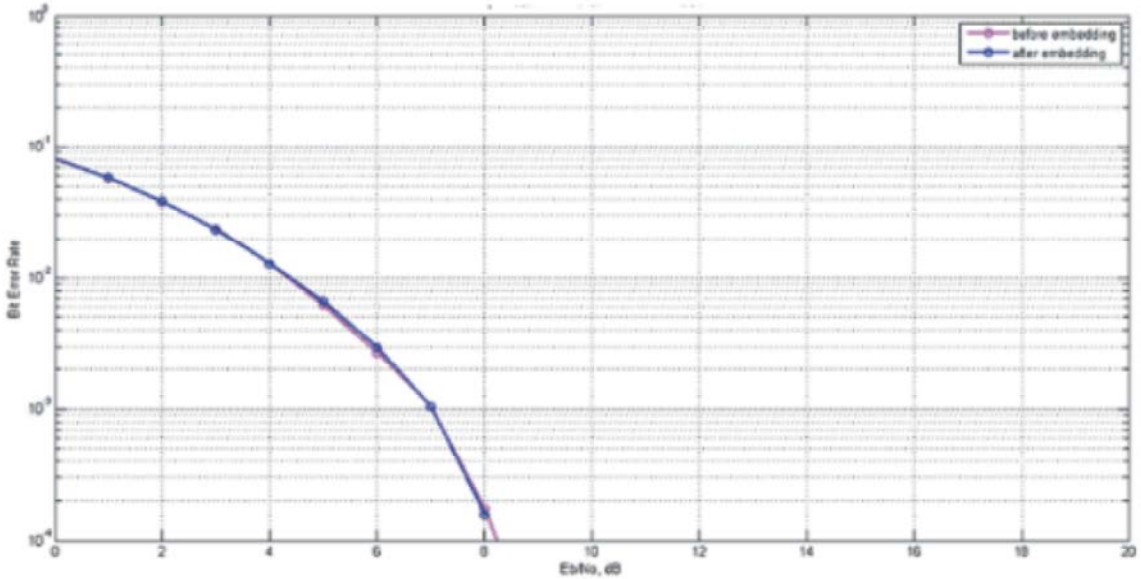

Fig. 5: Turbo code concatenated with convolutional code

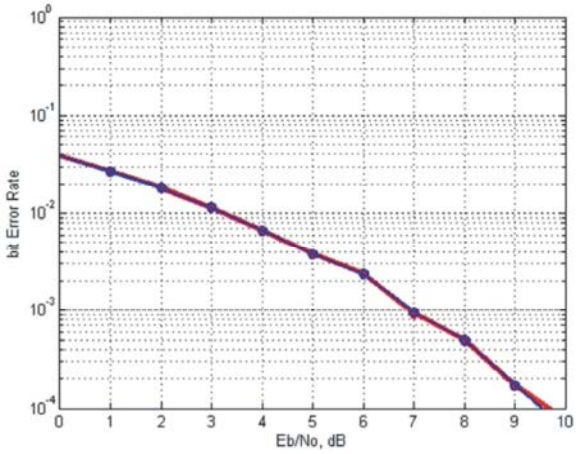

Fig. 6: Turbo code concatenated with alamouti code

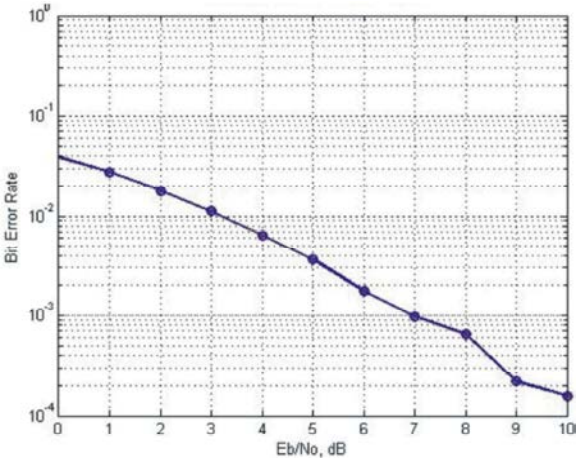

Fig. 7: Convolutional code concatenated with alamouti code

Hence proper choice of modulation scheme and error control code combats noise noise and the embedding of tag in FEC combats PUEA.

Figure 5 shows the system with and without embedding. Here turbo code concatenated with convolutional code is used as error control code. Concatenated error control coded offers much coding gain than individual codes. Hence it is more suitable for places where the noise is severe. The inclusion of tag takes care of the PUEA. There is no variation in the BER of the system with and without embedding.

Figure 6 shows the system with and without embedding. Here turbo code concatenated with alamouti code is used. Concatenated error control code takes care of the channel noise and alamouti code offers diversity.

Figure 7 shows the system with and without embedding. Here convolutioanl code concatenated with alamouti code is used. There is no variation in the BER of the system.

REFERENCES

1. León, O., J. Hernández-Serrano and M. Soriano, 2010. Securing cognitive radio networks, International Journal of Communication Systems, 23: 633-652.
2. Parvin, S., S. Han, B. Tian and F.K Hussain, 2010. Trust-based authentication for secure communication in Cognitive Radio Networks, International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, pp: 589-596.

3. Parvin, S., F.K. Hussain, O.K. Hussain, S. Han, B. Tian and E. Chang, 2012. Cognitive radio network security: A survey, Journal of Network and Computer Applications, 35: 1691-1708.
4. Zhang, C., R. Yu and Y. Zhang, 2012. Performance analysis of Primary User Emulation Attack in Cognitive Radio networks., International Wireless Communications and Mobile Computing Conference, pp: 371-376.
5. Kim, H. and K.G. Shin, 2008. In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?, ACM international conference on Mobile Computing and Networking, pp: 14-25.
6. Liu, Y., P. Ning and H. Dai, 2010.Authenticating primary users' signals in cognitive radio networks via integrated cryptographic radio networks via integrated cryptographic and wireless link signatures, IEEE Symp. on Security and Privacy, pp: 286-301.
7. Chen, R., J. Park and J.H. Reed, 2008. Defence against primary user emulation attacks in cognitive radio networks, IEEE transactions on Selected Areas in Communications, 26: 25-37.
8. Parvin, S., F.K. Hussain and O.K. Hussain, 2012. Digital signature-based authentication framework in cognitive radio networks, International Conference on Advances in Mobile Computing and Multimedia, pp: 136-142.
9. Kumar, V., J.M. Park, J. Kim, A. Aziz, 2012. Physicallayer authentication using controlled inter symbol interference, International Symposium on Dynamic Spectrum Access Networks, pp: 286.
10. Ruiliang Chen, Jung-Min Park and Jeffrey H. Reed, 2008. Defense against Prim ary User Emulation Attacks in Cognitive Radio Networks, IEEE transactions on Selected Areas in Communication, 26: 25-37.
11. Tingting Jiang, Huacheng Zeng, Qiben Yan, Wenjing Lou and Y. Thomas Hou, 2012. On the Limitation of Embedding Cryptographic Signature for Primary Transmitter Authentication, IEEE transactions on Wireless Communication Letters, 1: 324-327.
12. He, Y., L. Xu and W. Wu, 2014. A local joint fast handoff scheme in cognitive wireless mesh networks, IEEE transactions on Security and Communication Networks, 7: 455-465.
13. Tan, Xi Kapil Borle, Du Wenliang and Biao Chen, 2011. Cryptographic Link Signatures for Spectrum Usage Authentication in Cognitive Radio, ACM conference on Wireless Network Security, pp: 79-90.
14. Andrew Viterbi, J., 1971. Convolutional Codes and Their P erformance in Communication Systems, IEEE transactions on Communication Technology, 19: 751-772.
15. Claude, Berrou and Alain Glavieux, 1996. Near optimum error correcting coding and decoding-turbo codes, IEEE Transactions on Communications, 44: 1261-1271.
16. Avila, J. and K. Thenmozhi, 2013. DWT highlighted concatenated multi band orthogonal frequency division multiplexing (MB-OFDM)-upgraded enactment, International, 5: 2155-2162.