Received: December 11, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Novel Chaotic Communication based Test Signal Approach for Identification of Primary User Emulation Attack in Cognitive Radio Networks

Shriraghavan Madbushi[1*] **Rajeshree Raut**[2] **Mulpuri Santhi Sri Rukmini**[1]

[1] *Vignan's Foundation for Science, Technology and Research, Guntur, A.P., India*
[2] *Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India*
* Corresponding author's Email: m.shriraghavan@gmail.com

Abstract: In this paper, a novel method for detection of Primary User Emulation Attack (PUEA) by tagging (adding tag bits) a test signal in chaotic communication is proposed. The tagged test signal is masked by the secondary user using Lorenz chaotic attractor and sent over the channel. However, it doesn't interfere with test signals of other secondary users. The Bit Error Rate (BER) analysis of the received test signal indicates whether the channel is free or is under PUEA. If the BER of the received signal is above the set threshold then it indicates an attack. Moreover, for the first time the concept of test signal to identify whether the channel is occupied by the primary user or an attacker is proposed. It is further suggested to compare the result of the proposed method with the database provided by Spectrum Bridge Inc. (SBI). It is worth mentioning here that the proposed method has made the use of the centralized control approach employed by the Federal Communications Commission (FCC) to combat PUEA. Simulation results in terms of the BER have been analysed and compared with other existing methods to show the efficacy of the proposed method.

Keywords: Primary user, Secondary user, Spectrum holes, White spaces, Cognitive radio, Tagging, Spectrum sensing, Chaotic communication, Three coupled system, Primary user emulation attack.

1. Introduction

Recently cognitive radio technology has enticed a lot of researchers to pursue research in this exciting technology of Wireless Communications. Cognitive Radio is witnessed as a powerful solution to the existing spectrum scarcity problem. The Federal Communications Commission (FCC) in its study reported that most of the spectrum is not utilized efficiently; some portion is over used, while other is overloaded. The reason for this inefficient utilization is the static assignment of the radio spectrum by the FCC. The FCC is thus considering opening up the frequency bands for use by other opportunistic users called *secondary users* as long as they do not cause interference to the legitimate/licensed users also known as *primary users.*

To avoid interference to the primary users, secondary users must monitor the spectrum, make its opportunistic use and must vacate the band as soon as the primary user arrives. This monitoring is referred to as *spectrum sensing*. The free spectrum is also known as *"white space"* or *"spectrum hole"*. Due to open air nature of cognitive radio there are several threats and it is necessary to consider them for normal operations. One of the most prominent attacks identified in literature is Primary User Emulation Attack [1, 2].

In this attack a malicious or selfish user wants to gain an unfair use of spectrum. It achieves this by mimicking the primary user's signals and transmitting those signals [8]. The cognitive users on the other hand will think that the incumbent user is using the spectrum although it is not. The malicious/selfish user here emulates the primary signal's behavior or the energy strength [14]. Thus, it becomes necessary to correctly detect the presence of the primary user and also identify that whether the network is under PUE attack or not. Cooperative

DOI: 10.22266/ijies2018.0430.07

sensing plays an important role in detecting PUEA. Cooperative spectrum sensing using fusion rules along with energy detection scheme is proposed in [5]. In [10] the authors have proposed cooperative sensing scheme in which the probabilities of a fake PUEA signal is estimated in presence as well as absence of incumbent signal and the total error probability is minimized making use of the parameters estimated. The PUE attack can be viewed as an authentication problem and cryptographic signature is the best choice. In [13] the authors have proposed a solution applying the advanced encryption standard (AES) to improve the security of chaotic cognitive radio (CCR) system. One important question here is how the receiver can be sure that the signal it received was actually sent by the incumbent (primary user) or it was sent by a malicious / selfish user?

Unfortunately the cryptographic techniques cannot be employed due to the FCC constraint which states that “no modification to the incumbent system (the primary user signal) should be required to accommodate the opportunistic use of spectrum by secondary user” [7, 11]. Thus, modification of primary user’s signal using cryptographic techniques is not allowed. In addition to the constraint put by the FCC, authentication is difficult at layers other than the physical layer. The authentication scheme should be transparent to the existing users so that the existing devices should still function as usual however they cannot authenticate the signals. The reason for such a regulation by the FCC is to reduce the cost borne by the primary user. Without this constraint the cost induced on primary users will be too high and they will be reluctant to participate [11]. Flexible workflow architecture may provide a solution to this problem [12].

The FCC has provided a solution to mitigate the Primary User Emulation Attack by employing a centralized control approach. It has suggested making use of the white-space database maintained by the Spectrum Bridge Inc. (SBI), the first certified TV white-space database administrator in the United States. This also ensures that there is no interference to the licensed primary users by the unlicensed secondary users. In this method provided by the FCC there will be a base station which will be connected to the unlicensed secondary users and as well as the TV white space database via the internet.

The secondary user makes a request to the database through the base station. The base station thus gets a list of all available channels and it provides this data to the secondary users requesting the database. The secondary user then selects a channel based on some predefined rules, offered channels and a suitable radio technology.

However, the two major drawbacks of this method are i. this method fails where there is no internet connectivity or unavailability of the base station and ii. long time is taken by the device to receive the list of available channels from the base station and this burdens the network. In the proposed scheme the concept of the test signal has been projected for the very first time. It is worth mentioning here that the method complies with the FCC constraint already stated earlier and there is no need to have knowledge of the primary user signal. The test signal is first tagged i.e., tag bits are added to the signal (tag bit=1) and then this signal will be transmitted using chaotic communication to identify the occupancy of spectrum. The result of the proposed method then can be compared with the white-space database maintained by the Spectrum Bridge Inc. (SBI) to identify the Primary User Emulation Attack. The paper is organized as follows: In section 2 we have introduced the chaotic communication and have studied the Lorenz chaotic attractor and the three coupled chaotic system. In section 3 tagging of test signal with and without chaotic encoding, and decoding is explained and the Bit Error Rate (BER) analysis is also done for BPSK and QPSK modulation schemes. It is also shown that tagging with chaotic communication improves the BER of the received signal. Further, section 4 discusses the concept of the test signal using chaotic communication for identification of Primary User Emulation Attack. In section 5 the comparison of the proposed work with existing techniques has been discussed and finally section 6 concludes the paper.

2. An introduction to chaotic communication

In the field of Wireless Communications, Chaotic Communication has also been a field of interest. The reason behind this interest is due to low power consumption and low complexity in design of hardware, robustness in multi-path fading environments, low probability of interception, and resistance to jamming. Besides this, chaotic communication provides better security, overcomes the physical constraints faced by wireless systems and thus, provides a better performance. Chaotic communications is based on the chaos theory that describes behavior of nonlinear systems [3, 9]. Such systems are highly sensitive to initial conditions. In literature chaotic signal detection is divided in two classes- detecting signals contaminated by

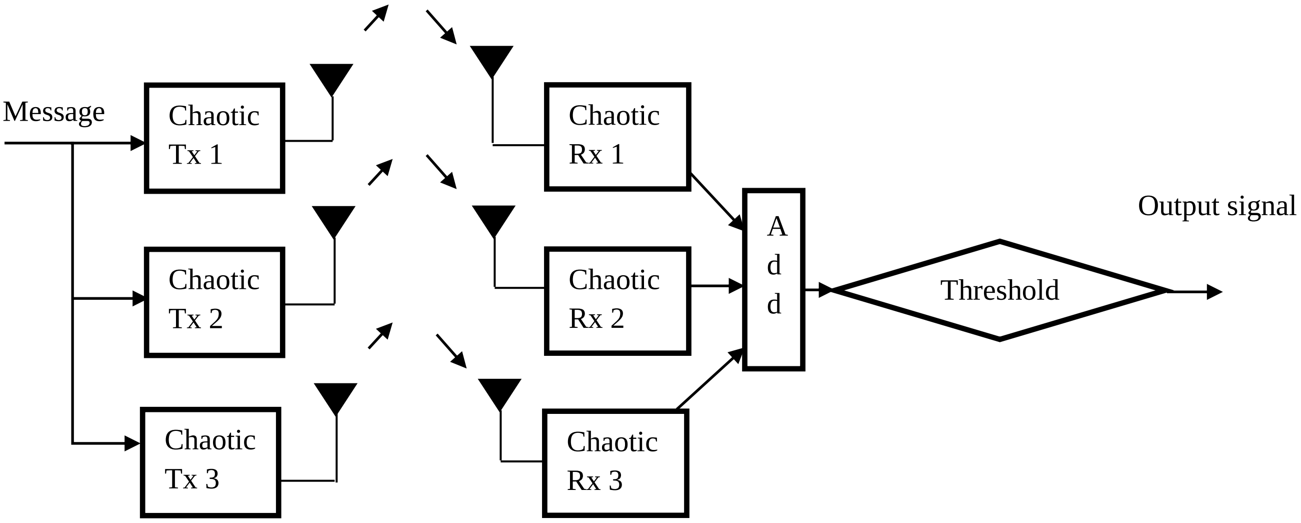


Figure.1 A three coupled wireless chaotic communication system [6]

chaotic signals and detecting signals contaminated by random noise. Chaotic signals are harder to identify, aperiodic and unstable. These signals have low power spectrum density and utilize larger bandwidth. There are numerous features of chaotic signals that make them attractive for use in wireless communications. It is theoretically proved that the Lyapunov exponents remain unaltered if a chaotic signal is utilized [9]. In [15] the authors have implemented frequency domain chaotic cognitive radio applying a chaotic sequence onto cognitive radio. They have further used universal software radio peripheral and GNU radio software for demonstration. In our study on chaotic communication for secure Wireless Communication we have implemented the method proposed in [6]. A chaotic system is described by the Eq. 1 shown below.

$$\dot{x} = A(x) + g(x) \qquad (1)$$

where, *A(x)* is the linear part and *g(x)* is the non-linear part of the system [6]. The chaotic system discussed here is a Lorenz's chaotic system. Its dynamic states are represented by the set of the following three equations as:

$$dx / dt = a\,(y-x) \qquad (2)$$
$$dy / dt = x\,(b-z)-y \qquad (3)$$
$$dz / dt = xy - cz \qquad (4)$$

where, *x, y* and *z* are the dynamic states, *a, b,* and *c* are constants greater than zero. We have analyzed one coupled, two coupled, and three coupled chaotic systems and have observed that the three coupled chaotic system's performance is the best. A three coupled system is as shown in Fig. 1.

In our experimentation, we found that when a signal is transmitted by a three coupled system the variance was 0.000000.The performance was also analyzed by BER versus the SNR plot. We also found that the variance for one coupled system is 0.110000, for two coupled system the variance is 0.020000. With this motivation we chose Chaotic Communication to propose a solution to combat the PUEA. The proposed work involves the concept of the test signal which is masked at first, encoded and decoded using three coupled Lorenz chaotic system, and the BER analysis to identify the channel state.

3. Analysis of proposed scheme and results (Part – I)

The PUE attack is at the physical layer of the cognitive network. The problem of validating the primary user can be viewed as spectrum sensing i.e., to identify whether the spectrum is currently occupied by the primary user or not. It is necessary to mention here that we are only interested in identifying the PUEA. The overall proposed work is divided in two parts (Part–I and Part–II). In Part –I the tagging scheme that is, inserting bits (tag bits) to a message signal is implemented. The message signal is then transmitted and further analysed in two ways, at first it is transmitted without chaotic communication and then, with chaotic

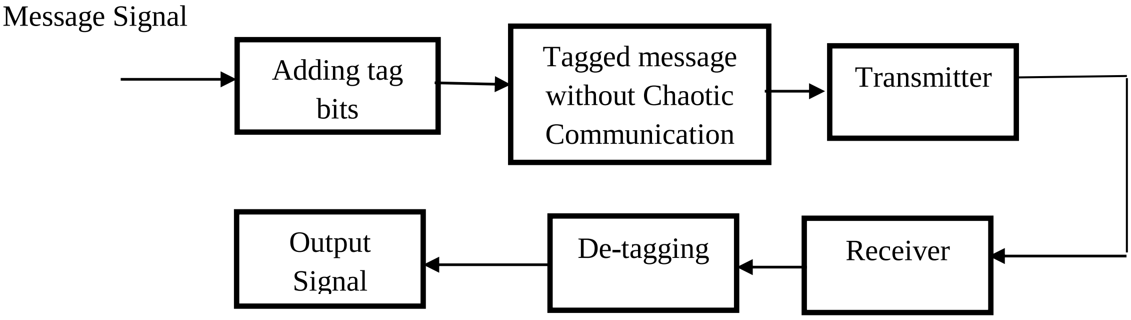


Figure. 2 Model with tagging and without chaotic communication

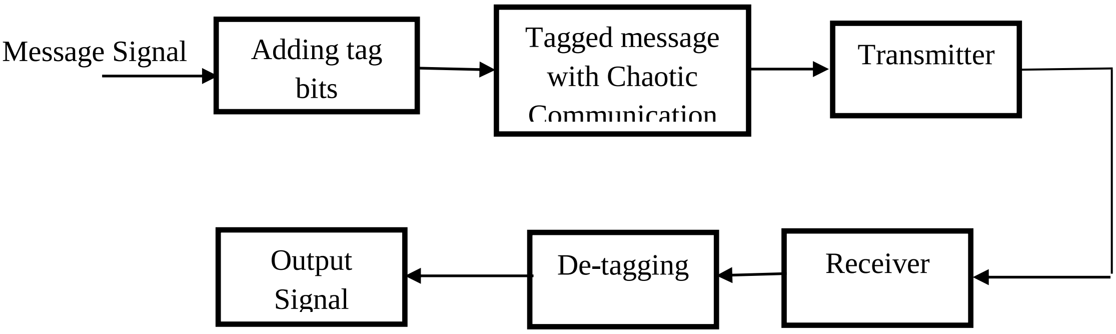


Figure.3 Proposed model with tagging and chaotic communication

communication. After implementing both the schemes the received signals were analysed by plotting the Bit Error Rate (BER) versus the Signal to Noise Ratio (SNR) curve plots. It was observed that the scheme of tagging with chaotic communication performs better than the scheme of tagging without chaotic communication.

The message signal is transmitted considering the Binary Phase Shift Keying (BPSK) as the modulation scheme. The code length of the message signal used is 1000 bits (it can be any number of bits, say, 100, 500, 1000, 2000).
The results for code length of 2000, 3000 and 4000 bits respectively are also observed.

Appending the tag bits is a simple procedure wherein the tag bits are inserted in the original message signal in a particular fashion. The procedure of appending the tag bits is shown in Fig. 4 and the process of chaotic encryption and decryption is explained later. Suppose that there are 20 bits (message bits) and tag bits have to be appended. The tag bit is appended after 1, 5, 9, 13th bit (odd position) and 2, 6, 10, and 14th bit (even position). The tag bit is denoted by 1. Thus, bit 1 is appended after bit number 13 and after bit number 14. Or, in other words bit 1 is inserted on both sides of bit number 14. In this way tag bits can be appended to any number of message bits. Note that the procedure continues and tag bits are appended till the end of message bits.

The tagging procedure can be made more secured by employing certain encryption algorithms or techniques. As already stated for chaotic encryption of the message signal three coupled chaotic system is used as shown in Fig. 1.

Fig. 2 and Fig. 3 represent the block diagrams of the proposed methods without and with chaotic communication using tagging. Further, the BER analysis is also done.

The new message (original message plus tag bits) is then masked by the chaotic state and transmitted. The encryption and decryption process at the transmitter and receiver is explained as in [6].

Encryption (master): $\dot{x} = Ax + g(x, v) + Lz_x$

where, $v = x_1 + M$

Decryption (slave): $\dot{y} = Ay + g(y,v) + Lz_y$

where $x \in R^n$, $y \in R^n$ are the state vectors, Ax and Ay denote the linear part, $g(x,v)$ and $g(y,v)$ denote the nonlinear part of this system. The controller gain of the system is denoted by L, and the coupling strength between master and slave system is denoted by K, (K > 0), z_x and z_y are the feedback signal.

20 bits - 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 (0s are in odd positions and 1s are at even positions)

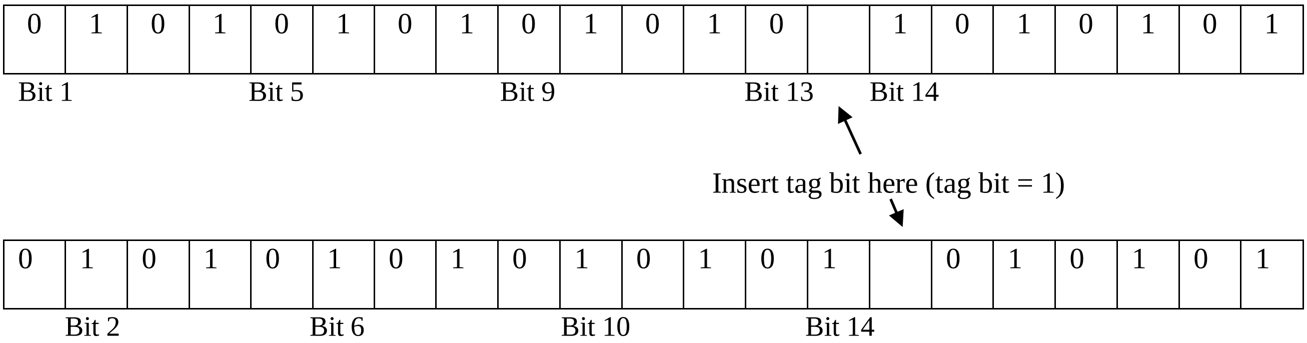


Figure.4 Inserting tag bits after bit 13 and bit 14

$x = [x_1 \;\; x_2 \;\; x_3]^T$, $y = [y_1 \;\; y_2 \;\; y_3]^T$,

$$A = \begin{bmatrix} -a & a & 0 \\ c & -(1+K) & 0 \\ 0 & 0 & -b \end{bmatrix}$$

$g(x,v) = [0 \quad -vx_3 \quad vx_2]^T$

$g(y,v) = [0 \quad -vy_3 \quad vy_2]^T$

$$L = \begin{bmatrix} l_1 \\ l_2 \\ l_3 \end{bmatrix}, \; z_x = M \text{ and } z_y = (v - y_1)$$

Here, $l_1 = -a$, $l_2 = a + c$ and $l_3 = 0$

The synchronization error and its error dynamic are defined as:

$$e = x - y = [e_1 \quad e_2 \quad e_3]^T$$

$$\dot{e} = \dot{x} - \dot{y} = Ae + g(x,v) - g(y,v) + L(z_x - z_y)$$

The main aim is to design L, the controller gain, such that the input message M can be received at the receiver. The message R that will be recovered is:

$R = v - y_1 = (x_1 + M) - y_1$

Here, as x_1 equals y_1 , $R = M$.

The chaotic system parameters used for the analysis are as follows:

$A = [0.1 \;\; 0.2 \;\; 0.3]$,

$M = [0.2 \;\; 0.1 \;\; 0.1]$,

$L = [0.15 \;\; 0.25 \;\; 0.35]$,

$x_1 = [0.22 \;\; 0.19 \;\; 0.43]$,

$z_x = [0.3 \;\; 0.6 \;\; 0.4]$

The following figure, Fig. 5 shows the signal of 20 bits in length transmitted and received using tagging and chaotic communication. It can be observed from Fig. 5 that the original sequence and the received sequence are almost the same and the tagged sequence and the received signal appear as noise.

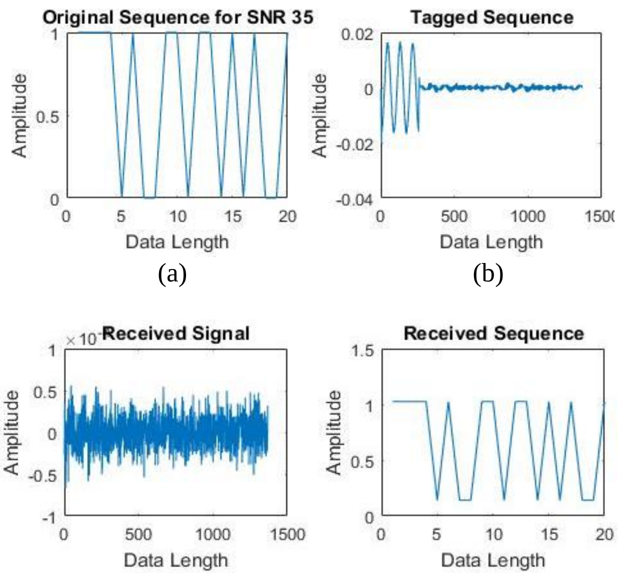
The chaotic constants must be same at the transmitter and the receiver side. It is difficult to recover the original signal unless the values of the chaotic constants are known and thus, they must be known to both transmitter and receiver for proper recovery of the signal.

Table 1 shows the comparison of Bit Error Rate (BER) with only tagging and BER with tagging and chaotic communication using BPSK.

It can be seen from Table 1 that the bit error rate is improved with tagging and chaotic communication as compared to only tagging. The Fig. 6 and Fig. 7 shows the bit error rate versus signal to noise ratio (BER vs SNR) curve for code length equal to 1000 bits using BPSK.

Table 1 also shows the percentage improvement for code length equal to 2000, 3000 and 4000 bits respectively.

Table 2 shows the comparison of Bit Error Rate (BER) with only tagging and BER with tagging and chaotic communication using Quadrature Phase Shift Keying (QPSK). It also shows the percentage improvement for code length equal to 2000, 3000 and 4000 bits respectively using QPSK as modulation scheme. The Fig. 8 and Fig. 9 show the bit error rate versus signal to noise ratio curve for code length equal to 1000 bits using QPSK. It can



(a) (b)

(c) (d)

Figure.5 Signal of 20 bits transmitted using tagging and chaotic communication

Table 1. Comparison of BER with tagging and tagging with chaotic communication using BPSK

Code length in bits	BER with only tagging	BER with Tagging and Chaotic Communication	% BER Improved
1000	5.4 x 10^{-4}	1.6 x 10^{-4}	70.3 %
2000	2.65 x 10^{-4}	8 x 10^{-5}	69.8 %
3000	1.75 x 10^{-4}	5.5 x 10^{-5}	68.57 %
4000	1.29 x 10^{-4}	4.2 x 10^{-5}	68.99 %

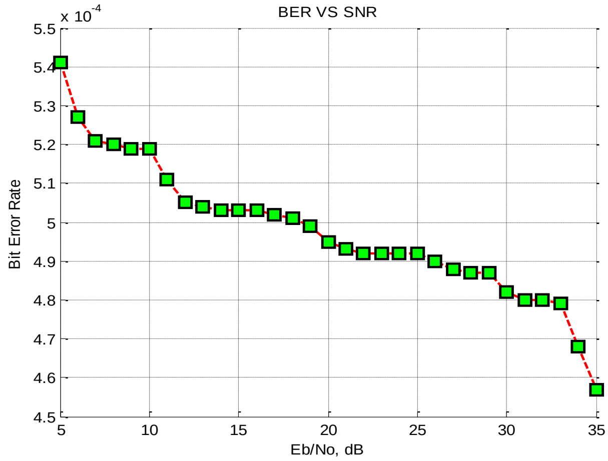


Figure. 6 BER vs SNR curve with tagging (code length = 1000 bits, BPSK)

be seen from Table 1 and Table 2 that there is an overall improvement of around 69 % in the Bit Error Rate (BER) of the received signal when we consider tagging with chaotic communication compared to only tagging using BPSK or QPSK.

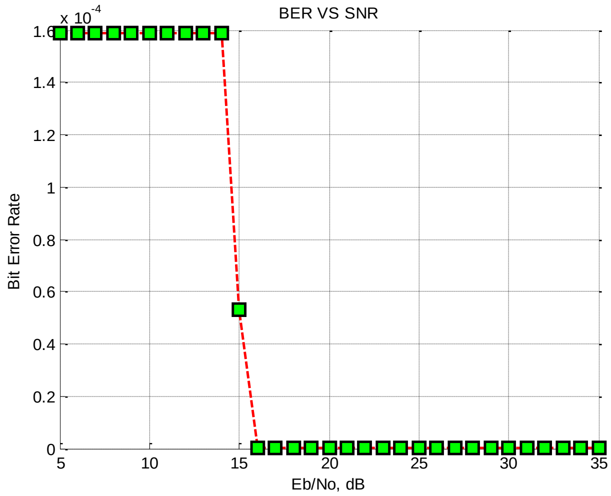


Figure.7 BER vs SNR curve with tagging and chaotic communication (code length = 1000 bits, BPSK)

Table 2. Comparison of BER with tagging and tagging with chaotic communication using QPSK

Code length in bits	BER with only tagging	BER with Tagging and Chaotic Communication	% BER Improved
1000	5.25 x 10^{-4}	1.601 x 10^{-4}	69.5 %
2000	2.59 x 10^{-4}	8.2 x 10^{-5}	68.33 %
3000	1.72 x 10^{-4}	5.5 x 10^{-5}	68.02 %
4000	1.29 x 10^{-4}	4.1 x 10^{-5}	68.21 %

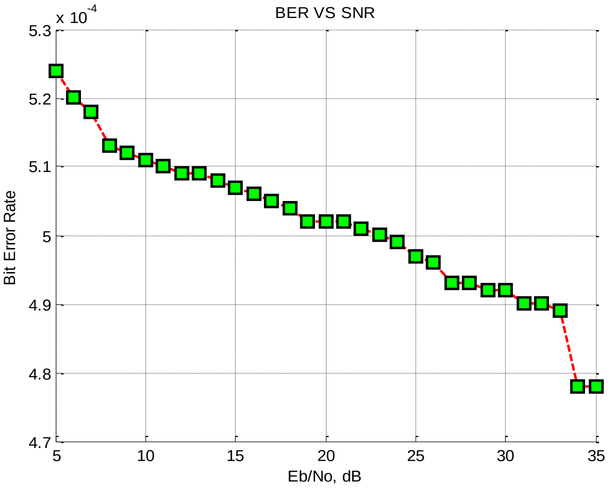


Figure.8 BER vs SNR curve with tagging (code length = 1000 bits, QPSK)

It may also be observed that the percentage improvement is not affected much even though the code word is changed from 1000 bits, to 2000 bits, 3000 and 4000 bits respectively. Thus, it can be

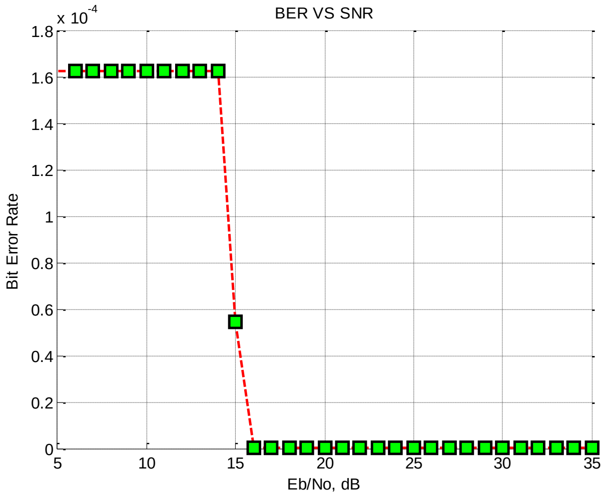


Figure.9 BER vs SNR curve with tagging and chaotic communication (code length = 1000 bits, QPSK)

concluded that BER has improved considerably when the signal is transmitted using tagging and chaotic communication. Moreover, the signal transmitted using chaotic approach appears as noise and thus provides more secure communication over wireless channel. The next section (Part-II) explains how the tagging scheme with chaotic communication is used to send the message/test signal over a channel and detect the Primary User Emulation Attack.

4. Analysis of proposed scheme and results (Part – II)

At this point, after observations and results from Part – I it was found that by using tagging and chaotic communication a signal is received and identified properly at the receiver. Also, it is a secured form of communication. In Primary User Emulation Attack (PUEA) one has to identify or differentiate between the original incumbent signal and the signal emulated by the malicious secondary user (attacker). Much work on Primary User Emulation Attack focuses on employing three methods mainly energy detection, cyclostationary feature detection, matched filter detection and so on.

Instead of identifying whether the signal is of primary user or some malicious secondary user (attacker) by using conventional methods of signal identification, the problem is analysed from a different angle. To the best of our knowledge for the first time we are proposing a solution wherein a test signal is sent over the channel to determine whether the channel is really occupied by the authentic Primary User or not. Moreover, no prior knowledge of primary user signal is required.

Whenever, a spectrum band is free it can be used by the secondary users as long as the primary user is not using it. Also, the band has to be vacated as soon as the primary user returns back. Now, if the band is free, the attacker may emulate a primary signal fooling and avoiding other secondary users to use the band.

In the proposed work a network of 20 users is simulated. During simulation the status of particular node is denoted as safe=0 or safe=1. Further it is assumed that the nodes denoted as safe=0 are attackers in the network. The transmission of test signal here takes place form a source node to destination node. Any node, irrespective of its status (safe=0 or safe=1) can communicate with any other node. When the test signal is transmitted from a source node whose status is safe=1 to a destination node whose status is either safe=0 or safe =1, the test signal is received properly at the receiver (BER < 0.7, threshold). This means that the channel/band is free and not under primary user emulation attack.

On the other hand if the test signal is transmitted from a source node whose status is safe=0 to a destination node whose status is either safe=0 or safe =1, the test signal is not received properly at the receiver (BER > threshold) and it can be concluded that the particular channel/band is under primary user emulation attack. Note that the noise is imminent. The proposed system continuously monitors the channel and scans for pre-decided patterns which are stored at the non-attacking secondary user nodes. These patterns are different for different secondary users, and the network router knows about them in advance.

In order to check if the band is free or not, the secondary user sends out its pattern, this pattern is encrypted using a 3-level chaotic encoder for security. The chaotic encryption process makes sure that the pattern behaves like a random noise sequence, and does not interfere with patterns of other secondary users. These two properties are fulfilled by selecting different and orthogonal values for the chaotic constants used in the encryption and decryption process.

Once the non-attacking or genuine secondary user transmits a chaotic sequence, it is decoded by the receiver/router. As the knowledge about the encryption constants is already known to the receiver/router, thus the sequence is decoded properly, with minimum to no errors. This ensures that the BER on the receiver side is either 0 or a minimum value. But, if an attacking node tries to access the channel, by transmitting any random sequences, then the receiver/router will not be able

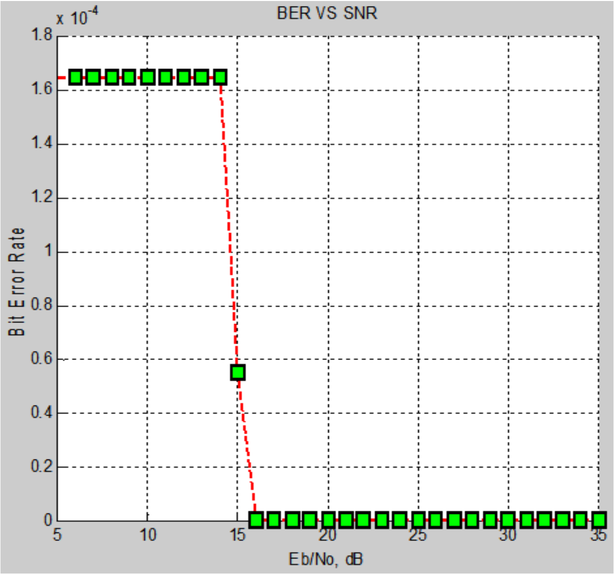


Figure.10 BER vs SNR curve for single attacker in network

to decode this sequence, and thereby the BER value between the known transmitted and unknown received signal will be very high, and the attacker would be marked. The following Fig. 10 below shows the bit error rate versus signal to noise ratio curve for a test signal of code length equal to 1000 bits transmitted using BPSK modulation scheme and a single attacker in network.

The detection rate accuracy obtained to identify the attack is 97%. For the same code length of 1000 bits and BPSK modulation and two attackers in the network the detection rate accuracy is 98.889%. And for three and four attackers in the network the detection accuracy is approximately 99% respectively. Further, it is suggested to compare the result obtained with the data base from Spectrum Bridge Inc. Note that the proposed approach has not used any database from Spectrum Bridge Inc. Thus, whenever a band is free a test signal is transmitted using tagging and chaotic communication (the procedure is same as explained earlier in Part-I) by the secondary user willing to use the band. At the end it is summarised that if the test signal sent by the secondary user transmitter is properly received at the secondary user receiver (BER less than or equal to a threshold value) then it is confirmed that the band is free and no attack has taken place. And if the BER of the received signal is greater than the set threshold then it is confirmed that an attacker is trying to emulate the primary user and the network is under Primary User Emulation Attack. One interesting thing to note here is that when the test signal is transmitted by using tagging and chaotic communication even the attacker will not know that a test signal is being transmitted to check the availability of the spectrum. This is because when the test signal is transmitted using chaotic communication the test signal appears as noise (see tagged sequence and received sequence in Fig. 5) and hence cannot be recognized by the attacker. As already stated in our work we further suggest the use of TV white space database maintained by Spectrum

Bridge Inc. the first certified TV white space database administrator in the United States. Thus, by using the proposed method of sending the test signal over a channel one can identify the occupancy of channel i.e., whether it is occupied or not and then the occupancy of the channel can be cross checked and verified by looking into the database. If the database shows that the channel is not occupied during a certain period of time and the result after employing our test signal method shows that the channel is occupied during the same period of time then it can be concluded that the network is under primary user emulation attack. On the other hand, if the database shows that the channel is occupied during a certain period of time and the result after employing our test signal method also shows that the channel is occupied during the same period of time then it indicates that the network is not under primary user emulation attack.

5. Comparison of our work with other existing techniques

This section discusses about the efficiency of the proposed method and the contribution towards providing a solution to mitigate Primary User Emulation Attack (PUEA). Many methods to mitigate the Primary User Emulation Attack are available in the literature. We just intend to show that our work is distinct from all those methods. To the best of our knowledge the concept of sending a test signal over the channel to check the channel availability is proposed for the first time. The proposed method is novel and hence its implementation results are the very first one to be obtained. We, however, compare and discuss the obtained results with other parallel methods for preventing the PUEA in terms of the BER. In our method we need not identify whether the signal sensed is of authentic primary user or emulated malicious user and then conclude whether the channel is really occupied by authentic primary user or not. One of the proposed methods is to deploy a helper node close to the primary user to authenticate the primary signal [7, 15, 17]. Our method does not recommend use of helper node placed in the close proximity of the primary user. This is one of the

Table 3. Comparison of BER values of the existing and the proposed method using BPSK

Eb/No (dB)	Ref. [18]	Ref. [15]	Ref. [17]	Proposed Method
1	8x10e-2	6x10e-2	8x10e-2	1.6x10e-4
2	5x10e-2	5x10e-2	7x10e-2	1.6x10e-4
3	3x10e-2	2x10e-2	5x10e-2	1.6x10e-4
4	2x10e-2	8x10e-3	2x10e-2	1.6x10e-4
5	8x10e-3	4x10e-3	8x10e-3	1.6x10e-4
6	5x10e-3	10e-3	5x10e-3	1.6x10e-4
7	9x10e-4	5x10e-4	10e-3	1.6x10e-4
8	2x10e-4	5x10e-5	10e-4	1.6x10e-4

Table 4. Comparison of BER values of the existing and the proposed method using QPSK

Eb/No (dB)	Ref. [18]	Ref. [15]	Ref. [17]	Proposed Method
1	7x10e-2	8x10e-2	8x10e-2	1.7x10e-4
2	5x10e-2	5x10e-2	6x10e-2	1.7x10e-4
3	3x10e-2	2x10e-2	4x10e-2	1.7x10e-4
4	2x10e-2	7x10e-3	10e-2	1.7x10e-4
5	7x10e-3	5x10e-3	8x10e-3	1.7x10e-4
6	4x10e-3	10e-3	3x10e-3	1.7x10e-4
7	8x10e-4	4x10e-4	10e-3	1.7x10e-4
8	8x10e-5	7x10e-5	2x10e-4	1.7x10e-4

distinguishing features of our work from others. In [11] the authors have suggested a method where the primary users are allowed to add a cryptographic link signature using modulation and coding. This however, violates the constraint put by the FCC. We wish to state here that our method not only follows the FCC constraint, but also makes use of the solution which the FCC has already suggested to mitigate PUEA. To further show our contribution we have analysed our method and the methods proposed in [7, 11, 15, 17, 18] and compared the results to show the effectiveness of our method. In [15, 17, 19] the authors suggested the generation of tag based PN sequence embedded in the forward error control codes or added in the code word or modulation scheme. This authentication tag is then sent by a helper node to the secondary user to identify about the presence or absence of the primary user. The performance is then evaluated by plotting the BER versus SNR curve before and after embedding the tag. In the Table 3, we compare the different BER values obtained against the different SNR values for our proposed chaotic communication method and the methods discussed in [15, 18, 19] where BPSK modulation scheme is used.

It is evident from the Table 3 that the proposed method performs well in terms of BER than other existing techniques. Table 4 compares the different BER values obtained against the different SNR values for the proposed chaotic communication method and the methods discussed in [15, 18, 19] where QPSK modulation scheme is used.

Lastly, it is observed that for both BPSK and QPSK modulation schemes the proposed chaotic communication based method overtakes other proposed methods in terms of the BER. The chaotic communication method is also economic as no helper node is needed in the proposed solution. Instead of employing a helper node we suggest the transmission of a test signal by the secondary user using chaotic communication technique, providing more security and proper identification of PUEA.

The Fig. 11 summarises the entire method based on tagging and chaotic communication.

6. Conclusion

This paper has explored a novel chaotic communication based approach to combat Primary User Emulation Attack in Cognitive Radio environment confirming to requirement of the FCC. Our approach incorporates the use of the test signal which is tagged at first and then encrypted by a 3-level Lorentz chaotic attractor and then transmitted to identify the channel occupancy state. The test signal of different secondary users will not interfere with each other as the selected chaotic constants are different, orthogonal and appear as random noise. There is no need of a helper node and this reduces the cost of the required infrastructure. We have analysed the performance of our scheme in terms of the BER and our simulation results indicate that the scheme outperforms other similar proposed schemes and improves the attack detection rate considerably. The detection rate obtained is greater than 95%.

Thus, we conclude that proposed method can be viewed as a potential solution to combat Primary User Emulation Attack. For our future work we propose to have a secured two layer mechanism based on Look Up Table (LUT) and chaotic communication for more accurate detection of the PUEA.

References

[1] R. Chen, and J.M. Park, “Ensuring trustworthy spectrum sensing in Cognitive Radio Networks, In: *Proc. of IEEE Workshop on Networking Technologies for Software Defined Radio (SDR’06),* pp. 110–119, 2006.

[2] R. Chen, J.M. Park, and J.H. Reed, "Defence against Primary User Emulation Attacks in Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 26, No. 1, pp. 25-37, 2008.

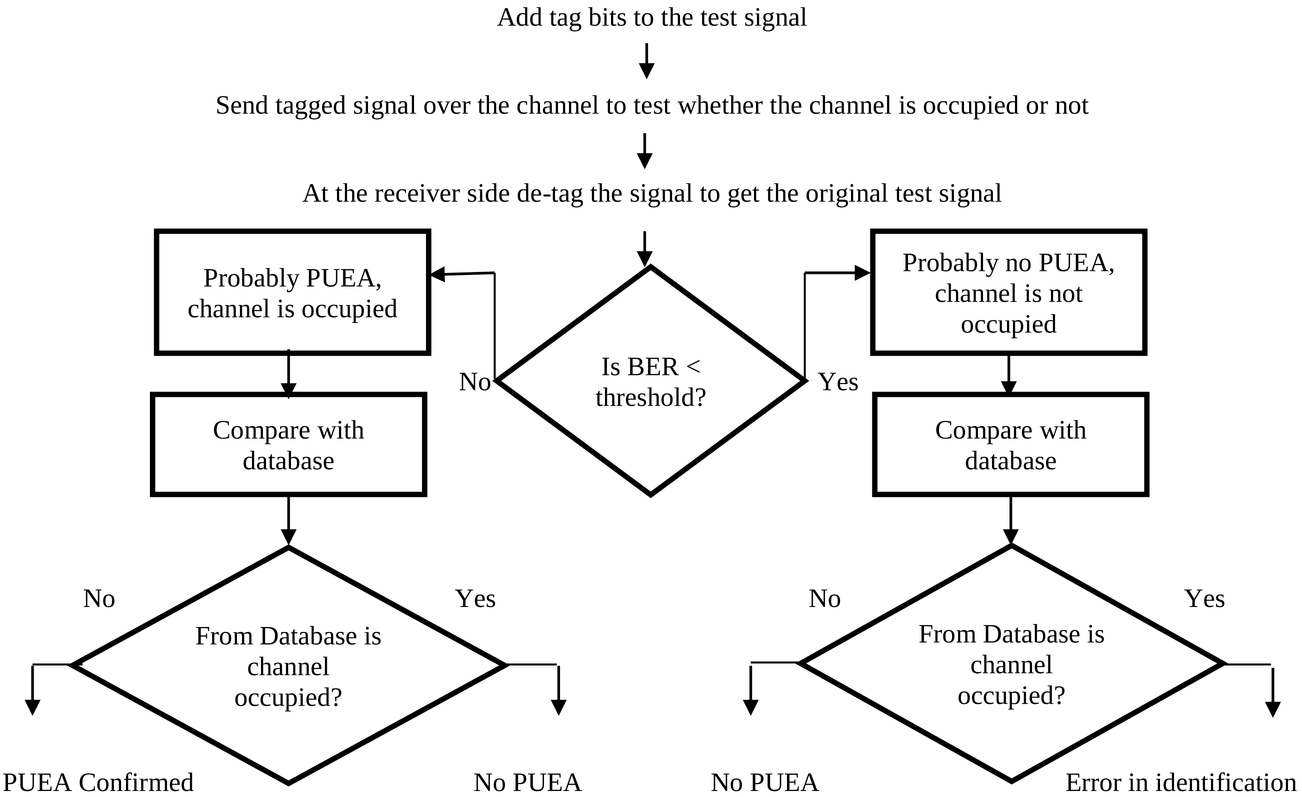

Add tag bits to the test signal
Send tagged signal over the channel to test whether the channel is occupied or not
At the receiver side de-tag the signal to get the original test signal
Is BER < threshold?
No
Yes
Probably PUEA, channel is occupied
Probably no PUEA, channel is not occupied
Compare with database
Compare with database
From Database is channel occupied?
From Database is channel occupied?
No
Yes
No
Yes
PUEA Confirmed
No PUEA
No PUEA
Error in identification

Figure.11 Flowchart showing the entire proposed method to detect PUEA

[3] J. Gu, S.H. Sohn, J.M. Kim, and M. Jin, "Chaotic Characteristic Based Sensing for Cognitive Radio", In: *Proc. of 5th International Conf. on Wireless Communications, Networking and Mobile Computing*, Beijing, pp. 1-4, 2009.

[4] M. Haghighat and S.M.S. Sadough, "Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks", In: *Proc. of Sixth International Symposium on Telecommunications (IST)*, Tehran, pp. 148-151, 2012.

[5] M. Haghighat and S.M.S. Sadough, "Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users", *AEU-International Journal of Electronics and Communications*, Vol. 68, No.6, pp. 520–527, 2014.

[6] H.H. Kuo, T.L. Liao, J.S. Lin, and J.J. Yan, "A New Structure of Chaotic Secure Communication in Wireless AWGN Channel", In: *Proc. of International Workshop on Chaos-Fractals Theories and Applications, (IWCFTA '09)*, Shenyang, pp. 182-185, 2009.

[7] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures", In: *Proc. of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, pp. 286-301, 2010.

[8] N. Nguyen-Thanh, P. Ciblat, and A.T. Pham, V.T. Nguyen, "Surveillance Strategies Against Primary User Emulation Attack in Cognitive Radio Networks", *IEEE Transactions on Wireless Communications*, Vol. 14, No. 9, pp. 4981-4993, 2015.

[9] A. Riaz, and M. Ali, "Chaotic Communications, their applications and advantages over traditional methods of communication", In: *Proc. of 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, (CNSDSP)*, Graz, pp. 21-24, 2008.

[10] A. A. Sharifi, M. Sharifi, and Mir Javad Musevi Niya, "Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach", *AEU-International Journal of Electronics and Communications*, Vol. 7, No. 2/3/4, pp. 95–104, 2016.

[11] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio", In: *Proc. of the fourth ACM Conf. on Wireless Network Security*, pp. 79–90, 2011.

[12] S.M. Tayade, and V. Chavan, "Challenges in Flexible Workflow Architecture: A Review", In: *Proc. of Fourth International Conf. on Emerging Trends in Engineering & Technology"*, Port Louis, pp. 39-42, 2011.

[13] L. Zhang, J. Yu, and Z. Wu, "Secured chaotic cognitive radio system using advanced encryption standard", In: *Proc. of IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications(PIMRC)*, Hong Kong, pp. 7-11, 2015.

[14] Y. Zheng, Y. Chen, C. Xing, J. Chen, and T. Zheng, "A scheme against primary user emulation attack based on improved energy detection", In: *Proc. of IEEE International Conf. on Information and Automation (ICIA)*, Ningbo, pp. 2056-2060, 2016.

[15] J. Avila, and K. Thenmozhi, "Error Control Code Based Resistance against Primary User Emulation Attack in Cognitive Radio", *Asian Journal of Scientific Research*, Vol. 8, No. 3, pp.324-332, 2015.

[16] R. Zhou, X. Li, J. Zhang, and Z. Wu, " Software defined radio based frequency domain chaotic cognitive radio", In: *Proc. of IEEE International SOC Conf.*, Taipei, pp. 259-264, 2011.

[17] J. Avila, and K. Thenmozhi, "Concatenated Error Control Code Based Authentication to Combat Primary User Emulation Attack", *Middle East Journal of Scientific Research*, Vol. 21, No. 9, pp.1498-1502, 2014.

[18] J. Avila, and M. Harini, "FEC Based Authentication to Combat PUEA in Cognitive Radio", *International Journal of Applied Engineering Research*, Vol. 9, No. 19, pp. 5731-5738, 2014.