Secure Communication in Cognitive Radio Networks

(Invited Paper)

Sugata Sanyal , Rohit Bhadauria and Chittabrata Ghosh

***Abstract*—Support for various multimedia applications in wireless networks demands additional bandwidth in the radio frequency spectrum. Efficient spectrum management algorithms are necessary to achieve immense success in wireless communications .Cognitive radio seems to be a panacea for increased utilization of licensed spectrum. It is defined as the new state of art technique that opportunistically share the licensed spectrum while imposing minimum interference to the licensed users. In this paper, we explore the adaptive characteristics of cognitive radio in secure and reliable communication. But the question is how to make the communication reliable such that there occurs no eavesdropping and information leakage. The possible solutions include integrating the merits of spread spectrum modulation, using encryption algorithms (public key and private key encryption), and its potential to switch over various frequency bands. In this paper, we focus on the various applications of cognitive radio and the numerous methodologies which enable a secure communication network.**

I. INTRODUCTION

Way back in 1999, Joseph Mitola [1] proposed the concept of cognitive radio. Cognitive radio (CR) is defined as a technical paradigm able to adapt itself dynamically to utilize the radio resources in the time, frequency, and space domains. A certain frequency spectrum is divided into smaller frequency bands. Each frequency band is allocated to licensed primary users. It has been observed experimentally that major portions of such frequency bands remain unused over substantial intervals of time. These unused portions of the spectrum are known as "spectrum holes" or "white spaces". The CR has the ability to utilize these spectrum holes effectively and intelligently while not imposing inadmissible interference to adjacent licensed primary users. For example: "TV White Spaces" in the television spectrum represent spectrum holes and are forseen to be used by the CR for the purpose of deploying supplementary wireless services. Because of its numerous characteristics and intelligent adaptation parameters, CR finds a lot of applications in the various fields demanding reliable and secure communication such as military applications, public safety applications [2]-[3], etc. It is their unique adaptability that makes the communication undetectable for external threats and hence allows the confidential conversations to be carried out in a secured way. Although in the present technological era, endless solutions are proposed towards the various security concerns that are the subjects of discussion among the whole scientific fraternity, but very few of them have been realized practically. These cognitive radios do suffer from a lot more number of challenges such as: on-neighbor discovery in the radio network, spectrum selection and sensing, detecting the user location and adapting itself to its demands etc. Cognitive radio, when combined with the spread spectrum modulation techniques, provide a highly secure communication format resistant to deliberate narrowband jamming and other obstruction tactics. Spread spectrum technique, because of its unique feature to make the data look like noise, is very much secure in the sense that the jamming and the interfering elements are unable to distinguish the data (mixed with noise) being sent over the channel and hence it may be a possible solution to avoid eavesdropping or information leakage. Even the various encryption techniques such as public key encryption (RSA, Elliptic, SHA) and private key encryption (DES, Triple DES, AES) algorithms can be used, in tandem, with cognitive radio to provide a form of secure communication. These encryption algorithms make sure that the key that is used at the transmitter side should be provided by the receiver (just like the pseudo-random sequence used in spread spectrum modulation) for correct information retrieval and hence ensures the security and also prevent the malicious users from taking control over the system, blocking the access to other secondary users. In this paper we have discussed the possible solutions towards providing a secure and reliable connection using cognitive radio along with spread spectrum modulation techniques and the various encryption techniques (symmetric and asymmetric).

Sugata Sanyal is with Tata Institute of Fundamental Research, India (sanyal@tifr.res.in).
Rohit Bhadauria, is with Vellore Institute of Technology, India (bhadauria.rohit@gmail.com).
Chittabrata Ghosh is with University of Washington, Seattle, WA, 98195, USA (ghoshc@u.washington.edu).

II. EVOLUTION OF SDR INTO CR

Software Defined Radio (SDR) [4] is defined as a radio
format in which the hardware components are realized by their software emulations and therefore called as software radios. CR technology is generally seen as the advancement of SDR in a more sophisticated manner making the sensing and adaptation parameters more

978-81-8465-152-2/09/$26.00 ©2009 CODEC

dynamic. Because of the paucity of these intelligent parameters, SDR suffers from the various spectrum management issues which CR has been successfully able to cope up with, and thus representing the functional development gained. Thus we can say that CR can be viewed as a combined application of SDR and intelligent signal processing with the functional elements of radio flexibility, spectral awareness and intelligent decision making.

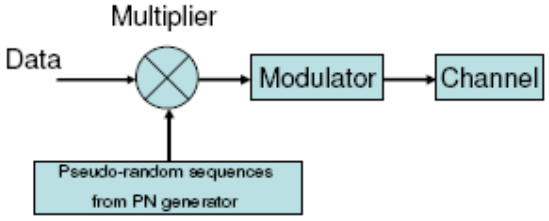

Fig. 1. Transmitter section in spread spectrum technique

III. NEED FOR SECURE COMMUNICATION

In this highly competitive world, the risks of economic and political espionage too have increased putting a lot of government and individual property at risk. A lot of techniques being used for carrying out communication are insecure in the sense that their security can be breached out and important conversations can be listened to or recorded. Even many of them don't require the authentication of the individual contacted. For example: the GSM services, though they provide good connectivity but they are prone to many security threats as discussed earlier. Even the standard mobile phones do not provide end to end security. Hence we can say that the secure communication is required to connect and provide transmission, processing, recording and monitoring for various purposes such as: secure telephone and network equipment and encryption management, secure data links to and from ground and satellite based remote platforms for real time information collection, communications between manned spaceflights, etc.

A. Possible solutions towards secure communication

Many existing technologies have such an ability that if combined with the cognitive radio technology can provide a communication format free from common security threats. Spread spectrum modulation format is one of them. Even the basic encryption technologies such as public key and private key encryption can be used in tandem with cognitive radio for such purposes. We will discuss the possibility of a secure communication format by using spread spectrum modulation technique with Cognitive radio. First, the basic spread spectrum modulation technique will be discussed.

B. Spread spectrum modulation

According to the standard definition: "Spread spectrum (SS) is a means of transmission in which a signal occupies a bandwidth in excess of the minimum necessary to send the information: the band spread is accomplished by means of a code which is independent of the data, and synchronized reception with the code at the receiver is used for de-spreading and subsequent data recovery". As shown in Fig. 1, the data signal is first multiplied with a pseudo-random sequence also known as spreading code and then modulated (generally using phase shift keying) and then transmitted over the channel. At the receiver side, as shown in Fig. 2, first the incoming signal is checked for some noise content (depending upon the noise characteristics of the channel) and if it contains some noise then the noise is removed first and then the signal is demodulated (based on the modulation technique

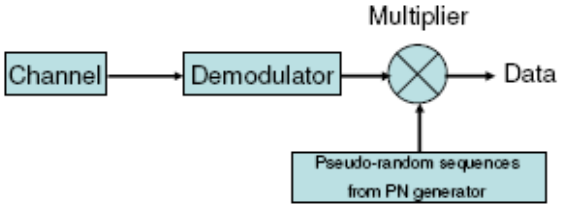

Fig. 2. Receiver section in spread spectrum technique

that has been used at the transmitter side). Now, the demodulated signal is multiplied with the same pseudo-random sequence that was used in the beginning and the final information signal is obtained. The receiver section is as shown below. Thus we see that in a SS technique, to retrieve the original signal being sent from the sender side, the knowledge of pseudo-random sequence is must. Moreover the data, having been multiplied with the PN sequence gets converted to a wide band signal gaining the shape and characteristics similar to noise. This unique feature of spread spectrum modulation technique makes it distinguishable from the other existing modulation techniques in such a way that it makes the data hidden among the random noise present or generated in the system and hence providing an escape from any third party (trying to sneak into the ongoing conversation). This quality of spread spectrum modulation algorithm can be exploited to provide a secure and reliable communication environment.

C. Encryption techniques

It has become a necessity to keep the data hidden from prying eyes in order to maintain security. And to achieve that various encryption techniques have been proposed such as: symmetric and asymmetric encryption techniques [5]. A symmetric encryption technique is also known as private key encryption algorithm. A few of such techniques are: RSA, Elliptic, SHA etc. In such a technique both sender and receiver have a private key, which they need to share before the transmission of the data gets started. What happens actually, the sender encrypts the data with the private key of the receiver and the receiver decrypts it using the same private key. Hence, such an encryption algorithm uses only a single key. But, in case of public key encryption (DES, Triple-DES, AES)technique we have two sets of keys associated with a user. Both sender and receiver have a set of public and private keys associated with them. These public keys are made accessible to the others over the network before the data transmission starts. Sender encrypts the data with the public key of the receiver and the receiver decrypts it using its own private key and this is how an asymmetric key algorithm operates. Although the private key encryption algorithms are fast but looking from the

978-81-8465-152-2/09/$26.00 ©2009 CODEC

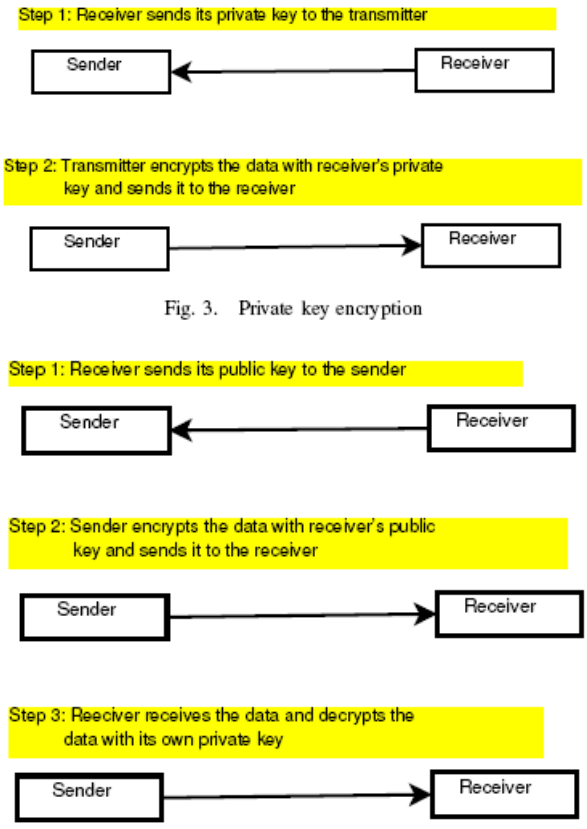

Fig. 3. Private key encryption

Fig. 4. Public key encryption

perspective of security obtained public key encryption techniques have an edge over the private key encryption algorithms. The private key encryption algorithm is as shown in Fig. 3. The public key encryption technique algorithm is as shown in Fig. 4. In public key encryption, there are three stages involved where as number of stages in a private key encryption algorithms are two.

IV. COGNITIVE RADIO IN SECURE COMMUNICATION

As per the IEEE 802.19 standard [6], the essential components of a cognitive radio network are the following:

- Incumbent user protection using spectrum sensing,
- White space database access,
- Security in accessing database and licensed spectrum, and
- spectrum sharing

For the perfect knowledge of the primary users in the licensed spectrum, the secondary users are projected to have access to white space database as in Fig. 5, i.e., database containing information of primary users in each and every licensed band. Federal Communications Commissions (FCC) has mandated spectrum sensing [7] along with access to this white space database. Spectrum sensing is a technique used by a CR to detect spectrum holes in the licensed spectrum. Existing research work have proposed use of physical layer and medium access control (MAC) layer characteristics of the primary user signal to detect such spectrum holes. The detection process, or rather spectrum sensing involves two types of errors: mis-detections (existence of a licensed user in one band is detected to be idle) and false alarms (an idle band is detected as an occupied band). The IEEE 802.19 standard

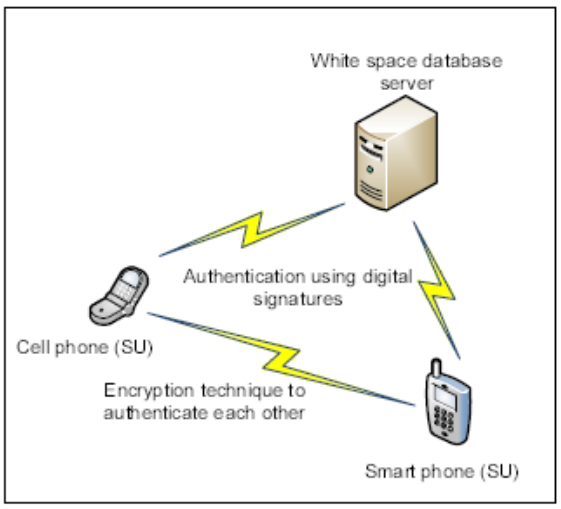

Fig. 5. Security in cognitive radio communication

is proposing a joint detection and access to the white space database for better spectrum sensing. But, two primary questions arises: (i) authenticate a CR before giving an exclusive access to the white space database and (ii) authenticate users in communication before sharing information about the white space database. Therefore, security in the context of cognitive radio networks is dealt in three stages:

- Step1: Authenticate a CR,
- Step2: Authenticate two users in communication, and
- Step3:Ensure security during the interval of communication between users.

In our paper, we consider all these stages of security envisioned and facilitated by a cognitive radio network.

A. Step 1: Authenticate a cognitive user

Authentication of a CR can be performed using digital signatures as in [5].

B. Step 2: Authenticate a cognitive user

Public and private key encryption techniques are used in authenticating CRs in communication.

C. Step 3: Secured cognitive communication

Once the CRs are authenticated, the next step is to ensure security in the information being shared. It is assumed that all the cognitive users have historic information about the primary user occupancy in the desired spectrum. In terms of the operation of a cognitive radio, an operational radio frequency spectrum is divided into N non-overlapping sub-bands. The set of sub-bands is denoted by Sub = {1, 2, . . . ,N}. Based on the historic information, it is further assumed that the probability of primary user occupancy in each sub-band is known to each cognitive radio. Let us define pi as the probability of the i^{th} sub-band being free at any instant of time. According to these sub-band free probabilities, the cognitive radio segregates the sub-bands into three different classes: small probability, large probability, and moderate probabilities of being free. The number of sub-

bands with small probabilities of being free are represented as $N_{free_{small}}$, with large probabilities as $N_{free_{large}}$, and with moderate probabilities as $N_{free_{mod}}$. The distribution of $N_{free_{small}}$ is as in [8] and the probability that there are k free sub-bands is

$$\begin{aligned} Pr(N_{free_{small}} = k) &\simeq \frac{{\lambda_s}^k e^{-\lambda_s}}{k!} \\ &= Pr_{Poi}(N_{free_{small}} = k), \quad (1) \end{aligned}$$

where $\lambda g = \Sigma_{i \in Sub_{small}} p_i$. This approximation follows a so-called Law of Rare Events. We further have the following lemma that gives an upper bound of the approximation error. The distribution of $N_{free_{mod}}$ in Sub_{mod} is as in [8] and the probability that there are k free sub-bands is:

$$\begin{aligned} Pr(N_{free_{mod}} = k) &\simeq \int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \frac{1}{\sqrt{2\pi C_n}} e^{-\left(\frac{(x-\overline{N}_{mod})^2}{2C_n}\right)} dx \\ &= Pr_{Normal}(N_{free_{mod}} = k), \quad (2) \end{aligned}$$

where n is the size of Sub_{mod}, k = 0, 1, · · ·, n, $N_{mod} = E[N_{free_{mod}}] = \Sigma_{i2Sub_{mod}} p_i$, and $C_n = \Sigma_{i2Sub_{mod}} p_i (1-p_i)$ represents the variance of $N_{free_{mod}}$.

The approximation of the distribution of $N_{free_{large}}$ follows essentially the path set by $N_{free_{small}}$. Note that $(1 - p_i)$ is small for i 2 Sub_{large}. Using the Law of Rare Events, the distribution of $N_{free_{large}}$ can also be approximated by a Poisson distribution. The following lemma facilitates computation of the probability distribution of $N_{free_{large}}$.

For k = 0, 1, · · ·, (N −m − n), we have

$$\begin{aligned} Pr(N_{free_{large}} = k) &\simeq \frac{e^{-\lambda_l} \lambda_l^{(N-m-n-k)}}{(N-m-n-k)!} \\ &= Pr_{Poi}(N_{free_{large}} = k), \quad (3) \end{aligned}$$

where $\lambda l = \Sigma_{i2Sub_{large}} (1-p_i)$. Therefore, the probability of k sub-bands being free at any point in time is given by:

$Pr(N_{free} = k)$

$$\begin{aligned} &= \sum Pr(N_{free_{small}} = k_1) Pr(N_{free_{mod}} = k_2) \\ &\qquad Pr(N_{free_{large}} = k_3) \quad (4) \end{aligned}$$

where the summation is taken over all $k_1 \geq 0$, $k_2 \geq 0$, and $k_3 \geq 0$ with $k_1 + k_2 + k_3 = k$.

With this preliminary knowledge, a cognitive user estimates a maximum probable number of free sub-bands available for its communication. The central idea of computing this probability is to compute the probable number of free subbands over which a cognitive radio switches during its communications. A cognitive user uses this information along with the information obtained from the white space database to comprehend the sequence of switching pattern for its communication. Once the two cognitive users have authenticated themselves to be genuine, the transmitting user conveys the switching pattern to its intended receiver. This procedure ensures that only the intended users are aware of the switching pattern of frequencies. Eavesdropping may lead to partial compromise of information to malicious users but not to its entirety.

D. Merging Spread Spectrum Modulation with Cognitive Radio

Cognitive radio technology when combined with the spread spectrum modulation techniques (such as Direct sequence, frequency hopping and time hopping) can provide a solution yielding secure communication. Although Cognitive radio technology is highly adaptive, continuously changing the frequency bands based on their availability, still such a system capable of monitoring the operational characteristics of a CR can be designed (by the interfering or jamming party) and hence transmission can be tracked. But with the combination of Spread spectrum modulation technique, the chances of transmission getting tracked are very less. In SS technique, the narrow band signal gets transformed into a wideband signal, on being multiplied with a pseudo-random signal (originally a wide band signal). This transformed wide band signal has the characteristics very much similar to the random noise signal present in the environment and hence it is very difficult by the intruding party to design such a system that could adapt itself with respect to the noise (as it is random) and hence the transmission remains unaffected by any sort of breaching-in effort.

V. CONCLUSION

In this paper, we have discussed the various features of cognitive radios that make them favorable for communication in an interfering environment. We also explored the possibilities of having a secure communication by merging the features of spread spectrum modulation techniques and encryption algorithms with the cognitive radio technology. We have also discussed the various fields and consumer applications where cognitive radio technology is applicable.

REFERENCES

[1] J. Mitola III, Cognitive radio: an integrated agent architecture for software defined radio. Ph.D. Thesis, Swedish Royal Institute of Technology,2000.

[2] S. Ball, A. Ferguson, and T. W. Rondeau, “Consumer applications of Cognitive Radio defined networks,” First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySpan’05, pp. 518-525, Nov. 2005.

[3] A. Gorcin and H. Arslan, “Public Safety and Emergency Case Communications: Opportunities from the Aspect of Cognitive Radio,” 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks,pp. 1 - 10, Oct. 2008.

[4] J. McHale, “Software defined radio communications: a spectrum of possibilities for military communications on the road to cognitive radio,” Military and Aerospace Electronics, http://mae.pennnet.com/display%5Farticle/369336/32/ARTCL/none/EXCON/

[5] C. N. Mathur and K. Subbalakshmi, “Digital signatures for centralized DSA networks,” Proc. First IEEE Workshop on Cognitive Radio Net- works, CCNC), Las Vegas, NE, Jan. 11, 2007.

[6] Y.-C. Liang, H.-H. Chen, J. Mitolla III, P. Mahonen, R. Kohno, and J.H. Reed, “Cognitive Radio: Theory and Applications,” IEEE Journal onSelected Areas in Communications, Vol. 26, No. 1, Jan 2008.

[7] K. Arshad and K. Moessner, “Collaborative Spectrum Sensing for Cognitive Radio,” IEEE International Conference on Communications Workshop, pp. 1-5, June 2009.

[8] C. Ghosh, Innovative Approaches to Spectrum Selection, Sensing, andSharing in Cognitive Radio Networks, PhD Thesis, University of Cincinnati, May 2009.