A Smart and Secure Wireless Communication System: Cognitive Radio

Shrikrishan Yadav, Santosh Kumar Singh, Krishna Chandra Roy

Abstract*— Trust is an important concept in human interactions which facilitates the formation and continued existence of functional human societies. The radio frequency spectrum is a limited natural resource and hence its efficient use is of the greatest importance. Cognitive radio is a smart wireless communication system that is conscious of its surrounding environment, learns from the environment and adapts its internal states by making corresponding changes in certain operating parameters in real time. In this paper, we search the adaptive characteristics of cognitive radio in secure and reliable communication. But how a communication system can be made reliable such that there occur no eavesdropping and information leakage. The possible solutions include integrating the merits of spread spectrum modulation, using encryption algorithms and it's potential to switch over various frequency bands. In the development of future wireless communication systems, the spectrum utilization will play an important key role due to the shortage of unallocated spectrum. The main tasks of the cognitive radio are to provide highly reliable communications whenever and wherever needed and how to utilize the radio spectrum efficiently. Cognitive radio can be the best communication system in an emergency condition as Earthquake, flood and Tsunami etc when all communication systems are failed to provide information and to communicate each other.

***Index Terms*—Decryption, Encryption, Primary User, Radio Frequency Spectrum, Secondary User, Spectrum Analysis**

I. INTRODUCTION

The electromagnetic radio spectrum is a natural resource and hence its use by transmitters and receivers is licensed by governments. The spectrum bands are usually licensed to certain services such as mobile, fixed broadcast and satellite to avoid harmful interference between different networks to affect users. Nowadays mostly spectrum bands are allocated to certain services but worldwide spectrum occupancy measurements show that only some portions of the spectrum band are fully used and rest of spectrum are unused.

Over the past few years, Cognitive Radio (CR) has been considered as a demanding concept for improving the utilization of limited radio spectrum resources for future wireless communications and mobile computing. Since a member of Cognitive Radio Networks (CRN) may join or leave the network at any time; the issue of supporting secure communication in CRNs becomes more critical than the other conventional wireless networks. This work thus proposes a secure trust-based authentication approach for CRNs. A CR node's trust value is determined from its previous trust behavior in the network and depending on this trust value. It is decided whether this CR node will obtain access to the Primary User's free spectrum or not. The security analysis is performed to guarantee that the proposed approach achieves security proof.

Cognitive radio adaptation engines use the concept of artificial intelligence i.e. machine learning techniques such as evolutionary algorithms or expert systems to adapt the transmission parameters of a wireless system in order to optimize the performance of the communication. The cognitive engine models the environment internally and uses relationships between the transmission parameters and environmental measurements to perform the adaptation.

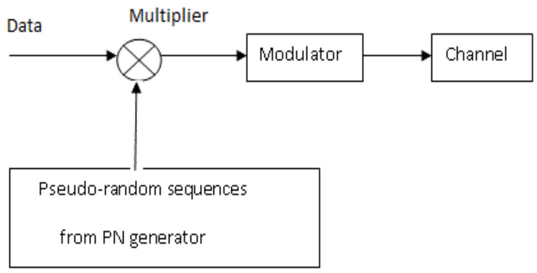

Figure 1. Transmitter section in spread spectrum technique

The selection of a suitable set of transmission parameters is a key to the design of a cognitive wireless system. Each additional parameter adds another dimension of control over the cognitive radio. We use a genetic algorithm based cognitive engine, and fitness functions to demonstrate how the optimality of the cognitive engine decision is affected when certain parameters are held constant and not allowed to be adapted by the cognitive engine. By comparing the resulting cognitive engine decisions, when they are not adapting specific parameters to those of systems that are fully adaptable, we identify the parameters that do not affect the outcome and can be disregarded in order to minimize the complexity of the system.

Cognitive radio, when combined with the spread spectrum modulation techniques, provides a highly secure communication format

Manuscript Received February 09, 2012.

Shrikrishan Yadav, CSE Department, PAHER University, Udaipur, India, 9694978211, (e-mail: shrikrishanyadav77@gamil.com).

Santosh Kumar Singh, IT Department, Gyan Vihar University, Jaipur, India, 9829813220, (e-mail: sks.mtech@gmail.com).

Prof. Krishna Chandra Roy, ECE Department, PAHER University, Udaipur, India, 9461588796, (e-mail: roy.krishna@rediffmail.com).

challenging to calculate narrowband jamming and other obstruction devices. 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 being sent over the channel and hence it may be a possible solution to avoid eavesdropping or information leakage.

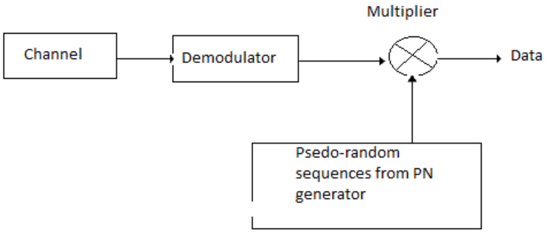

Figure 2. Receiver section in spread spectrum technique

For the above said purpose, the various encryption techniques such as public key encryption (RSA, SHA) and private key encryption (DES, AES) algorithms can be used 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 for correct information retrieval and hence ensures the security and also prevent the malicious users from taking control over the system and 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 either symmetric or asymmetric.

II. NEED FOR SECURE COMMUNICATION

Nowadays to maintain privacy has become essential for unauthorized or authorized users. In this highly competitive world the risks of economic and political surveillance 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 and important conversations can be listened to or recorded by other person. 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 laying on your front to many security threats as known to everyone. 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, which is better for data or information security etc.

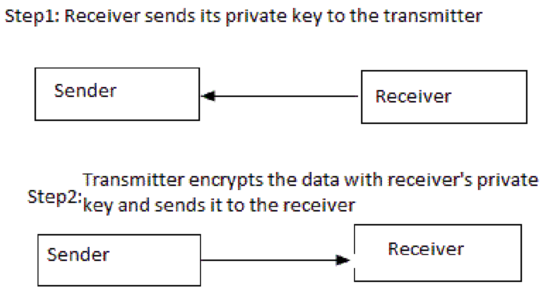
Step1: Receiver sends its private key to the transmitter
Sender
Receiver
Step2:
Transmitter encrypts the data with receiver's private key and sends it to the receiver
Sender
Receiver

Figure 3. Private Key Encryption

A. Possible solutions towards safe and sound communication

There are many existing technologies which have such ability that if they 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 cycle with cognitive radio for such purposes as shown in fig. 4.

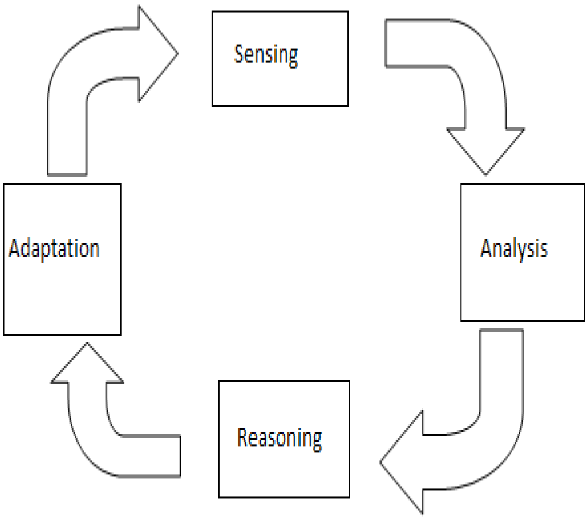

Figure 4. Cognitive Radio Cycle

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 and transmitted over the channel.

At the receiver side, as shown in Fig. 2, at first the incoming signal is checked for some noise content and if it contains some noise then the noise is removed first and then the signal is demodulated. 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. 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 presented or generated in the system and hence providing an escape from any third party. This quality of spread spectrum modulation algorithm can be exploited to provide a secure and reliable communication environment and also for better and convenient communication in the wireless system.

C. Some encryption techniques

There are various encryption techniques have been proposed such as: symmetric and asymmetric encryption techniques. A symmetric encryption technique is also known as private key encryption algorithm. A few of such techniques are: RSA, 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. In this technique, 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, and 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.

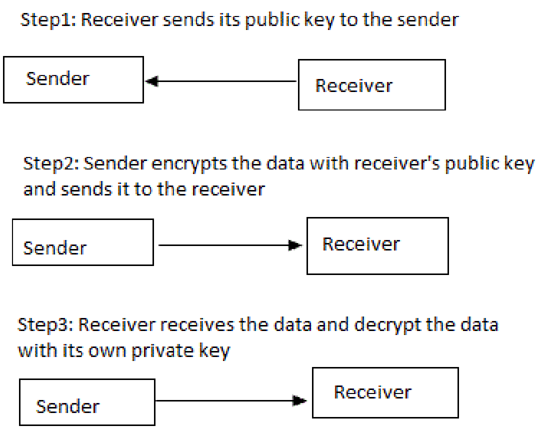
Step1: Receiver sends its public key to the sender
Sender
Receiver
Step2: Sender encrypts the data with receiver's public key and sends it to the receiver
Sender
Receiver
Step3: Receiver receives the data and decrypt the data with its own private key
Sender
Receiver

Figure 5. Public Key Encryption

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 perspective of security obtained public key encryption the 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. 5. In public key encryption, there are three stages involved where as number of stages in a private key encryption algorithms are two.

III. COGNITIVE RADIO IN SECURE AND SOUND COMMUNICATION

As per the IEEE 802.19 standard, the essential components of a cognitive radio network which are:

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

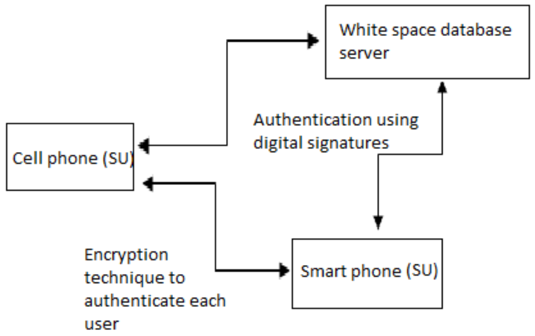
White space database server
Authentication using digital signatures
Cell phone (SU)
Encryption technique to authenticate each user
Smart phone (SU)

Figure 6. Security in cognitive radio communication

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. 6, i.e., database containing information of primary users in each and every licensed band. Federal Communications Commission’s (FCC) has mandated spectrum sensing 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 works 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: mix-detections and false alarms.

Therefore, security in the context of cognitive radio networks is dealt in three stages:

•Step1: Authenticate a CR

•Step2: Authenticate two users in communication

•Step3: Ensure security during the interval of communication between users.

IV. CONCLUSION

It has become an essential to keep the data hidden from snooping eyes in order to maintain security. This can be achieved by using various encryption techniques, which have been proposed such as: symmetric and asymmetric encryption techniques. In this paper, we have discussed the various features of cognitive radios that make them favorable for communication in an interfering environment and for secure communication. 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.

ACKNOWLEDGEMENTS

We would like to express our gratitude to experts Dr. K. K. Chabdda, (Director, PCE), Associate Professor Santosh Choudhary, (HOD, CSE Department), and other members of CSE Dept. for their guidance and contributions. We would also like to thank for the valuable information's they provided us. We would like to thank our family members for their love and care. At last but least we would like to thank everyone, just everyone!

REFERENCES

1. Federal Communications Commission, " Spectrum Policy Task Force ," Rep. ET Docket no. 02-135, Nov. 2002.
2. P. Kolodzy et al., "Next generation communications: Kickoff meeting," in Proc. DARPA, Oct. 17, 2001.
3. M. McHenry, "Frequency agile spectrum access technologies," in FCC Workshop Cogn. Radio, May 19, 2003.
4. G. Staple and K. Werbach, "The end of spectrum scarcity," IEEE Spectrum, vol. 41, no. 3, pp. 48–52, Mar. 2004.
5. J. Mitola et al., "Cognitive radio: Making software radios more personal," IEEE Pers. Commun., vol. 6, no. 4, pp. 13–18, Aug. 1999.
6. J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Doctor of Technology, Royal Inst. Technol. (KTH), Stockholm, Sweden, 2000.
7. A. Ralston and E. D. Reilly, Encyclopedia of Computer Science. New York: Van Nostrand, 1993, pp. 186–186.
8. R. Pfeifer and C. Scheier, Understanding Intelligence. Cambridge, MA: MIT Press, 1999, pp. 5–6.
9. M. A. Fischler and O. Firschein, Intelligence: The Brain, and the Computer, ser. MA. Reading: Addison-Wesley, 1987, p. 81.
10. B. Fette, "Technical challenges and opportunities," presented at the Conf. Cogn. Radio, Las Vegas, NV, Mar. 15–16, 2004.
11. J. Mitola, Ed., "Special issue on software radio," in IEEE Commun. Mag., May 1995.
12. Software Defined Radio: Origins, Drivers, and International Perspectives, W. Tuttlebee, Ed., Wiley, New York, 2002.
13. Software Defined Radio: Architectures, Systems and Functions,M.Milliger et al., Eds., Wiley, New York, 2003.
14. FCC, Cognitive Radio Workshop, May 19, 2003, [Online].Available: http://www.fcc.gov/searchtools.html.
15. Proc. Conf. Cogn. Radios, Las Vegas, NV, Mar. 15–16, 2004. York: Springer-Verlag, 1999.
16. T. R. Shields, "SDR Update," Global Standards Collaboration, Sophia Antipolis, France, Powerpoint Presentation GSC10_grsc3(05)20, 28 August - 2 September 2005.
17. P. Kolodzy, "Definition of Cognitive Radios." Hoboken, NJ: Wireless Network Security Center (WiNSeC) of the Stevens Institute of Technology, 2005.
18. K. Nolan and J. Grosspietsch, "Cognitive Radio WG," SDR Forum, Brussels, Belgium, Powerpoint Presentation 14 September 2005.
19. Digham, F., M. Alouini, and M. Simon. 2003. On the energy detection of unknown signals over fading channels. Proc. IEEE Int. Conf. on Communications. 5: 3575-3579.
20. Digham,F., M. Alouini, and M. Simon. 2007. On the Energy Detection of Unknown Signals Over Fading Channels IEEE Transactions on Communications 55: 21-24
21. P. Mannion, "Smart radios stretch spectrum," in Electronic Engineering Times (EETimes), vol. 2006: A Global Sources and CMP joint venture, 2006.
22. www.ebooksdownloadfree.com/.../cognitive-radio-technology-Bruce Fette.

AUTHOR PROFILE

Shrikrishan Yadav: working as an Assistant Professor in Computer Science and Engineering Department in PAHER University, Udaipur, India. He has completed B. E. in computer science and engineering from Mohanlal Shukhadia University, Udaipur and pursued M.Tech. in Information Communication from Gyan Vihar University, Jaipur. He has more than two years of teaching experience. He is also published and presented 9 papers in International and National journals and conferences. He is an associate member of Computer Society of India (CSI), a member of International Association of Engineers (IAENG), International Association of Engineering and Scientists (IAEST) and International Association of Computer Science and Information Technology (IACSIT). His current research interest includes Cognitive Radio, Wireless Sensor Networks, Artificial Intelligence, Information Communication etc.

Santosh Kumar Singh: received his B.E. degree in Electronics and Communication Engineering from S. J. College of Engineering, under Mysore University, Karnataka, India, year 1995 and M.Tech in Information Technology in 2004. He having 13 year teaching experience and pursuing his Ph.D. degree in Engg. at the School of Engineering, Suresh Gyan Vihar University, Jaipur, India. He published one book and one paper in well-reputed publication. He is also presented several papers in International and National conference. His current research interests include next generation wireless networks, wireless sensor networks and industrial embedded system.

Prof. Krishna Chandra Roy: received his M.Sc. (Engg.) degree in from NIT Patna, Bihar, India and Ph.D degree in "Digital Signal Processing in a New Binary System" year 2003. He has currently professor & Principal in Pacific College of Technology Udaipur, India and having more than 15 year teaching and research experiences. He guided many Ph.D scholars. He is also published and presented more than 55 papers in International and National journals and conferences. He published two books Problems & solution in Electromagnetic Field Theory by Neelkanth Publishers (p) Ltd., Year-2006 and Digital Communication by University Science Press, Year-2009 respectively. His current research interests include Digital Signal Processing and wireless embedded system.