Chapter 70
Analysis of Primary Emulsion Attack in Cognitive Radio Using Distributed On-Demand Routing Protocol

Neelaveni Rangaraj and Sridevi Balu

Abstract The aim of this chapter is to design a novel framework for cognitive radio to overcome the security-based challenge by considering authentication and confidentiality. Particularly, the chapter focuses on the primary emulation attack, as it gives the authentication for the unlicensed user to use the unused the spectrum. These unlicensed users are considered as the secondary users and to authorize to use the spectrum only for the required period without compromising the security of the primary user. The distributed on-demand routing protocol is used in cognitive radio, and hence it can be used for the group of users sharing the same spectrum. RSA with the distributed on-demand routing protocol yields a secure key for sharing that particular session within the users. A comparison between the classical protocols for generating the secret key with Diffie–Hellman algorithm and other protocols is also done in this work by analyzing their vulnerabilities**.**

Keywords Distributed on-demand · RSA algorithm · Authentication · Spectrum sharing

Abbreviations

ACK	Acknowledgment
CBS	Cognitive Base Station
CR	Cognitive Radio
CRV	Credit Risk Value
CS	Cognitive Sensing
DORP	Distributed On-Demand Routing Protocol
DSDV	Destination Sequenced Distance Vector

N. Rangaraj (✉)
MNM Jain Engineering college, Chennai, Tamil Nadu, India

S. Balu
Velammal Institute of Technology, Chennai, Tamil Nadu, India

L. Ashok Kumar et al. (eds.), *Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications*,
https://doi.org/10.1007/978-3-030-24051-6_70

PU Primary User
PUE Primary User Emulsion
RSA Rivest Shamir and Adleman (Public Key Encryption Technology)
ZRP Zone routing protocol

70.1 Introduction

Cognitive Radio can change its transmitter parameter based on interaction with the environment in which it operates. It comprises of licensed user as well as unlicensed user. Its characteristics are spectrum sensing, spectrum analysis, and spectrum decision. The spectrum-sensing techniques in cognitive radio transmitter include cyclo-stationary-based detection, energy detection, and matched filter detection. Matched filter detection sensing is performed by correlating the observed signal with the known sample to detect the presence of primary users. Sensing the energy of the signal with the estimated and the limited value is the energy detection method. The limited value indicates the channel can be used by the user. The drawback is that it cannot distinguish between signals of the primary user from those of the secondary user. Cyclo-stationary-based detection is used for detecting periodicity of the received signal. One of the sensing techniques is the cooperative sensing technique which is further classified as centralized and decentralized spectrum technique in which former is a cluster head or server that collects the sensing information and transmits this information to control the cognitive radio traffic. The distributed sensing is in which cognitive nodes inform the other nodes which are in the same group to choose the spectrum. Hybrid sensing is very similar to distributed system sensing. In this technique, when the primary user arrives, it vacates the channel immediately without informing other nodes. The primary user as a licensed user gives permission to access the spectrum for the secondary users. When the secondary user acts as a primary user using the identity of the primary user to know about the detailed information about the spectrum, then it is said to be the primary emulsion attack.

70.2 Previous Works

Mandakini Gupta et al. [1] described primary user emulsion (PUE) attack as one of the most important threats of spectrum sensing for wireless cognitive radio network. Based on the wireless signal, a PU is detected in a given band, and all secondary users should avoid accessing that band. However, when a secondary user is detected, other secondary users may choose to share that same band. In a primary user attack, a malicious secondary user tries to gain priority over the secondary user by transmitting signals that emulate the characteristics of primary user. In this chapter, the radio

software of a cognitive radio is modified to change its emulsion characteristics (i.e., modulation, frequency, power, etc.) so that the emulsion characteristics resemble those of a PU.

R. Akhila et al. [2] analyzed that in a wireless ad hoc network, the spectrum will not be sufficiently used. The licensed user can use the licensed spectrum who is said to be the primary user, whereas the unlicensed user can use the spectrum when the licensed users are not using it. This authentication to the unlicensed user must be given in a proper manner to maintain the secrecy of the data. The unlicensed secondary users may transmit and restore the fake information about the spectrum for its future use, thus causing a danger to the message spread through the spectrum to the primary user. Those secondary users will be known as the selfish users. They will degrade the network performance. Here, a method which uses credit risk value (CRV) is being proposed to identify the selfish users to improve the network performance and efficiency.

Rohit Chakravarthy et al. [3] also described primary user emulation (PUE) attack as one of the major concerns and problems in cognitive radio networks. In this chapter, a primary use authentication scheme is proposed to solve the PUE attack problem by employing an underlay RF fingerprint in the primary user signal. Specifically, an underlay waveform is introduced on the top of the header of the legitimate primary user signal. As a result, the underlay waveform exhibits a unique and different cyclo-stationary feature than the primary user signal. The PUE attack signal, on the other hand, will not reveal this cyclo-stationary feature and fail the authentication. Throughput Maximization in Cognitive radio networks [4], Security enhancement using key agreement protocols [5], analysis of the sensing techniques in CR network [6], and the Primary emulation attack rectification by physical layer network coding [7] are explored.

70.3 Proposed Work

This chapter focuses to enhance the security of primary user during the primary emulsion attack in a cognitive radio network. Cognitive radio (CR) is the enabling technology for supporting dynamic spectrum access. The functionality of cognitive radio includes the characteristics of power, modulation techniques, to find its geographic location using the transceiver to form a group of nodes, sensing the spectrum for the primary user, implementing the key exchange methodology for a secured communication, and to make it applicable for mobile applications.

To represent these functions of CR, a group of nodes are created for representing the communication in CR. The cognitive base station (CBS) acts as a central medium for communication. CBS finds a cognitive sensing (CS) which is an optimum node for communication in each group of nodes as shown in Fig. 70.1. Each group comprises of primary and secondary users who in a real-time example can be differentiated by the cost as licensed and unlicensed users. When the primary user wants to communicate, the access is taking place through cognitive sensing. The RSA algorithm is used in the authentication process between a cognitive

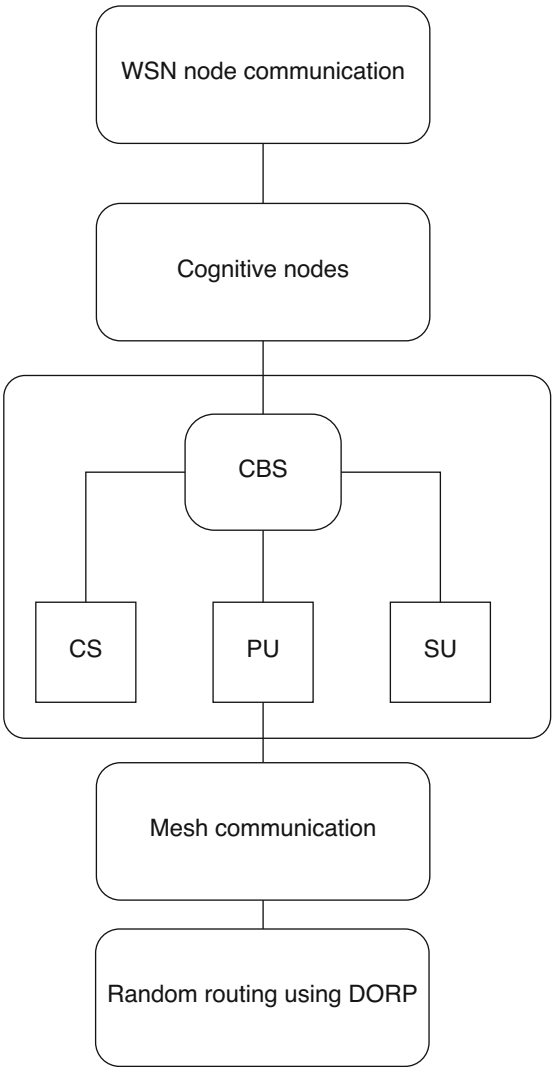

Fig. 70.1 Basic block diagram

sensed node and a primary user. Similarly, between CS and CBS, the encryption and decryption of messages take place using this algorithm. When the primary user is not using the spectrum (spectrum underutilization), secondary users communicate via primary user by the same authentication process. Though CR has been proposed as a promising solution for improving spectrum utilization, the major drawback is the primary emulsion attack. In CR network, primary users have priority over secondary users when accessing the wireless channel. The primary emulsion attack is said to happen when a malicious secondary user exploits this spectrum access acting as a primary user. This has to be avoided to achieve a successful communication. Hence, we introduce a group-leader technique to secure the primary user.

70.4 Implementation

The implementation of the security enhancement of the cognitive radio is done with the help of network simulator.

70.4.1 Initial Setup

When the nodes are randomly deployed, the communication is carried out using the destination sequenced distance vector algorithm. This algorithm is similar to the distance vector algorithm in which the routing table is updated periodically, where each node informs about its neighboring node and there by forming the network topology. In DSDV, sequence number is used to avoid the formation of loop. Though this routing is carried out, the efficiency in communication is hindered by the primary emulsion attack, where the secondary users try to gain priority over the primary user by transmitting signals that emulate the characteristics of the primary users.

70.4.2 Distributed On-Demand Routing Protocol

In Distributed On-Demand Routing Protocol (DORP), the cumulative delay between the end nodes is calculated by determining the delay in each route. Hence, the best distributing path is found using this protocol. The added advantage of this routing technique is an improved range for communication as shown in Fig. 70.2.

70.4.3 RSA Algorithm

Key exchange between the CBS and the primary user plays the vital role in the security enhancement of the cognitive spectrum which prevents the primary emulsion attack. The public key generated by the RSA algorithm in the CBS is decrypted in the primary user using the private key. When there is a mismatch in the key between them then it is said to be an attack by the secondary user. If the key matches, then the authentication to use the spectrum can be given to the user who generated the key. The following steps are followed for the public key generation in CBS.

Step1: Select two prime numbers p and q.
Step2: Calculate $n = p*q$.
Step3: Calculate $\phi(n) = (p-1)*(q-1)$.
Step4: Select a variable e (for encryption) in which it should satisfy the condition $1 < e < \phi(n)$.

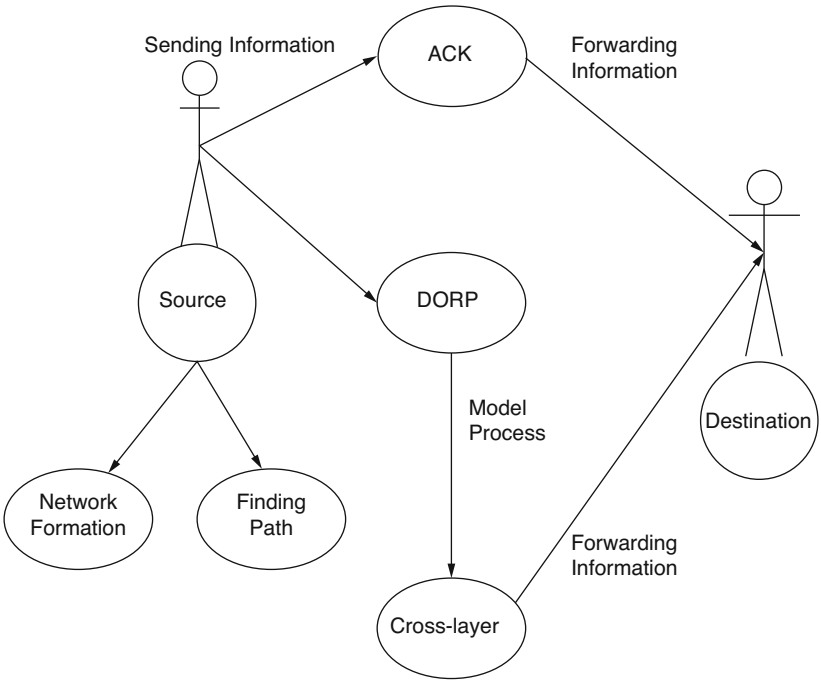

Fig. 70.2 Functional diagram of distributed on-demand routing protocol

Step5: Calculate d such that d∗eMod ϕ(n) = 1.
Step6: For calculating private key Kr = {d,n}is used.
Step7: For calculating public key Ku = {e,n}is used.
Step8: For encryption the plain text M should be less than n.
Step9: Cipher text C in CBS can be calculated by $C = M^e$ (mod n).
Step 10: For decrypting the plain text $M = C^d$(mod n).

70.5 Comparisons

The Diffie–Hellman algorithm is the better option for an insecure communication channel, even when there is no interchange of keys or messages in between the end users. However, the RSA algorithm is used for the channel to secure the user authentication as because of their symmetric key exchange methodology as a digital signature which is little faster than the Diffie–Hellman algorithm. Even though the RSA algorithm has various advantages, it can be used for applications like an emergency which considers without the possibility of usage of other spectrums. However, for military applications, the Diffie–Hellman algorithm can be used for asymmetric key exchange.

The mobile ad hoc protocols are classified into table-driven and on–demand-driven protocols. As the spectrum for the user will be selected only when needed, distributed on-demand protocols are used, even though the table can be maintained for the primary user, each time CBS need not store the routing loops as it may lead to insecure communication. The hybrid, zone routing protocol (ZRP), can be used as it is applicable for versatile environments. However, the significance of ZRP is the usage for wide range of area. As this chapter concerns only a short range, and keeping the parameters payload and latency, Distributed On-Demand Protocol is preferred over the Zone Routing Protocol (ZRP).

70.6 Conclusions

The purpose of this chapter is to give a new user some basic idea of how the simulator works, how to set up simulation networks, where to look for further information about network components in simulator codes, how to create new network components, etc., mainly by giving simple examples and brief explanations based on our experiences. Although all the usages of the simulator or possible network simulation setups may not be covered in this project, the project should help a new user to get started quickly.

References

1. Gupta M, Jain A, Soni A (2016) A survey: render of PUE attack in cognitive radio compressed by software defined radio. IEEE, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp 4029–4034,
2. Priyadharshini RA, Haimavathi KU (2016) Detection of attacks and Countermeasures in cognitive radio network. International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp 1102–1106
3. Chakravarthy R, Huang K, Zhang L, Wu Z (2017) Primary user authentication of cognitive radio network using underlay waveform. Cognitive communications for aerospace applications workshop, pp 1–5
4. Wang CL, Chen HW, Tsai ZY (2012) Throughput maximization for cognitive radio networks with wideband spectrum sensing. IEEE wireless communications and networking conference, pp 1293–1298
5. Vizvari S, Berangi R, Nematollahi K (2016) Authentication and authorizing scheme based on UMTS AKA protocol for cognitive radio network. IEEE KBEI, pp 118–123
6. Zheng J, Chen C-H, Cheng J-y, Shi L (2009) Cognitive radio: methods for the detection of free bands. IEEE Int Conf Netw Secur Wireless Commun Trust Comput 2:343–345
7. Gope J, Dutta P, Bhadra S, Das S, Jana S, Dalmia N, Choudhury S (2017) Analytical study of primary user emulsion attack detection techniques in cognitive radio ad hoc network. IEEE 8th annual ubiquitous computing, electronics and Mobile communication conference (UEMCON), October, pp 392–395