A Comparative Study of Software Defined Radio and Cognitive Radio Network Technology Security

Awanish Kumar Kaushik
Electronics and Telecommunication Deptt.
Vishveshwarya Group of Institutions, Dadri
Gr. Noida, India
awanishkkaushik@gmail.com

Abstract—Software Defined Radio (SDR) and Cognitive Radio (CR) are fast technologies, which can be used to reduce the spectrum shortage problem. The modern software defined radio has been called the heart of a cognitive radio. The applications executing on the radio differentiate a cognitive radio from a software-defined radio. Additional hardware in the form of sensors and actuators increases the more cognitive radio applications. Cognitive radio networks have become an increasingly part of the wireless networking landscape due to the increasing scarcity of spectrum resources. A number of wireless applications have been developing over the last decade. Government agencies give the license to most of the frequency spectrum, such as Federal Communications Commission (FCC). The main objective of this paper is to analyze the SDR based Cognitive radio, threats and security issue of the main recent advancements and architectures of Software Defined Radio and cognitive radio networks.

Keywords—Software Defined Radio (SDR), Cognitive Radio (CR), Threats, Protections.

I. INTRODUCTION

Software Defined Radio (SDR) and Cognitive Radio (CR) technology have revolutionized our opportunities in wireless communications. To increase the spectral utilization and to optimize the use of radio resources is the main motivation behind this technology. Cognitive radio based on software defined radio (SDR) is viewed as a good solution for a wide number of wireless communication problems, e.g. spectrum under-utilization, geo-location and networking applications [1]-[2]. Joseph Mitola coined the terms “cognitive radio” and “software defined radio” in his 2000 PhD dissertation [3].

The concept of SDR has evolved from the seminal work of Joseph Mitola in [4]. Over this period a number of references have provided their definition of SDR, which has developed to various types of interpretations of what SDR actually is and what is not. The main reason is that SDR is the key term, which may be applied to a wide range of radio platforms and their concepts. In ETSI [5], SDR is defined as “radio in which the radio frequency (RF) operating parameters including, but not limited to, frequency range, modulation type, or output power can be set or altered by software, and/or the technique by which this is achieved”. An alternative definition is provided by the SDR Forum, now named Wireless Innovation Forum [6], which has developed a definition of SDR in cooperation with IEEE working group P1900.1: “Radio in which some or all of the physical layer functions are software defined”.

The design and deployment of CR and SDR have been investigated in a number of papers and research studies starting from the paper of Joseph Mitola [7]. Architecture for a rapidly deployable radio network using software defined radio techniques was presented in [8]. The mobility of such network was limited due to the size of the software radio system. Recent advancements in semiconductors and other enabling technologies have made it feasible to build small form factor software radios using different computing devices [9]-[11].

The flexibility and inter-operability of software radio systems are managed by different architectures, e.g. Software Communication Architecture (SCA) [12]. Although this practice facilitates modular paging of radio systems using object-oriented design principles, it suffers from computational overhead caused mainly by hardware abstraction managed by Common Object Request Broker Architecture (CORBA) [13].

Cognitive radio [14], [15], inclusive of software-defined radio, has been proposed as the means to promote the efficient use of the spectrum by exploiting the existence of spectrum holes. Moreover, we may infer from Pfeifer and Scheier [16] that the
A Comparative Study of Software Defined Radio and Cognitive Radio Network Technology Security

interdisciplinary study of cognition is concerned with exploring general principles of intelligence through a synthetic methodology termed learning by understanding. By putting these ideas together and keeping in mind that cognitive radio is targetted to improve the utilization of radio spectrum.

In addition to the cognitive capabilities, it is also for reconfigurability, this latter capability is provided by a platform which is software-defined radio, upon which a cognitive radio is made. Software-defined radio (SDR) is a practical reality today, thanks to the convergence of two key technologies: digital radio, and computer software [17]–[19].

This paper presents a summary analysis of Software Define Radio and Cognitive radio security concept. The paper is structured as follows. Section II presents the cognitive Radio functions. Section III presents the block diagram of Software-defined radio (SDR), in section IV, V, VI, VII define the cognitive radio network, Software-defined radio (SDR) and Cognitive Radio threats, protection against Software-defined radio (SDR) and Cognitive Radio threats and summary and conclusions are drawn in section VIII.

II- COGNITIVE RADIO FUNCTIONS

CRs must provide the following functions:-
1) Determine which portions of the spectrum are available and detect the presence of licensed users who operates in a licensed band (spectrum sensing).
2) select the best available channel (spectrum management) for communication.
3) Coordinate access to this channel with other users (spectrum sharing).
4) Vacate the channel when a licensed user is detected (spectrum mobility).
These functions are dependent on each other as seen in Figure 1.

The figure (1) describes the relationships among the various functions. For example:- spectrum mobility could alert the spectrum sensing function on detected alters in the spectrum environment. By acting on the alert, the spectrum sensing function can collect the knowledge of the spectrum environment and give it to the spectrum management function to re-plan for the allocation of spectrum bands.

The disruption of spectrum sensing has an impact on the other functions due to the needed information is not performed by them effectively. Spectrum management needs the knowledge of the spectrum environment acquired to select the best available channel by spectrum sensing. Spectrum sharing requires the information on the bands selected by spectrum management function in each node. CR networks are defined by many nodes, with different capabilities, which interact on the basis of defined protocols and policies.

A survey of CR networks and the related architectures is presented in [20], where the authors describe the various CR techniques and architectures to implement SDR and CR networks. The two most common approaches are called as collaborative and uncooperative are:-

1) **In the collaborative approach**, the cognitive functions are based on the coordination of the CR nodes, which exchange information to optimize the spectrum utilization to improve the efficiency of the network.
2) **In the uncooperative approach**, each CR node implements the cognitive functions on its own.

The collaborative approach is usually considered more efficient, faster to converge to shared spectrum resources allocation and more reliable than the uncooperative approach but it requires common channels to exchange information. The common channel is often called Cognitive Control Channel (CCC) [21] and it is responsible for distributing the cognitive messages in the CR network. In a centralized solution, a central node, e.g. a base station (BS), controls the allocation of the spectrum resources or collects the spectrum sensing information. A centralized solution may be more efficient but the central node can be represented as
a single point of failure. A comparison between the centralized and distributed approaches for spectrum management is presented in [22].

III- SDR BASED COGNITIVE RADIO NETWORK

The proposed cognitive radio architecture is divided in 3 sub-systems, as shown in Figure- 2:
1) Configurable digital transceiver.
2) Channel monitoring and spectrum sensing module.
3) Communication management and control.

The communication management sub-system uses spectrum sensing module and feedback from the channel monitoring to adjust the operation parameters in the RF front end and digital transceiver. The configurability of cognitive radio is governed by the design of the configurable digital transceiver. Adaptability is maintained by the second and third subsystems.

Figure 2- Cognitive Radio Architecture

The RF front-end has input parameters which includes amplifier gains, operation frequency, and channel filters’ bandwidth. The input parameters of the digital transceivers processing chain is identified by the input parameters of the digital transceivers.

The digital wireless transceiver typically has a chain of function blocks which is described by physical layer specifications of their wireless standard, i.e., sampling rate, modulation, and coding scheme. Each standard is broken into a combination of digital signal processing blocks, such as filters, signal transforms, and logical and arithmetic operations.

The output parameters of the configurable transceiver are the performance measures maintained by cognitive radio. The wide arrows in Fig.1 represent high speed data paths. One path is from the digital transceiver to the spectrum monitoring. Another path is found between the digital transceiver and I/O devices, as well as between the digital transceiver and communication management and control sub-system. The communication management and control sub-system performs several main tasks in the cognitive radio design.

IV- COGNITIVE RADIO NETWORK (CRN)

Consider the network model, a primary network is an existing network infrastructure operating with license in a given spectrum band, shown in fig 3 such as current cellular or TV broadcast networks, and offers its services to the primary users. A CRN works in both licensed and unlicensed bands. When using the licensed band, the CRN may coexist with existing primary networks, and that’s why it is seen as a secondary network. The selection of a given channel for the operation of the CRN is based on sensing measurements performed by the CRN members in two possible manners: (1) centralized (base station of an infrastructure mode network) and (2) cooperative, (ad hoc networks).

The information is propagated through the CRN by means of either an in-band channel or out-of-band channel relates the new frequencies. One of the most studied solutions is the use of a cognitive pilot channel (CPC) [23]. This channel is ideally predefined and used between all the CRN members.
A Comparative Study of Software Defined Radio and Cognitive Radio Network Technology Security

Figure 3- Cognitive Radio Network (CRN)

Many approaches have been proposed in the literature, such as the IEEE 802.22 [24], DIMSUMnet [25], KNOWS [26], CORVUS [27], or DSAP [28]. Among them, it is discussing the IEEE 802.22 defines a point-multipoint air-interface, composed by a base station and several consumer premise equipments.

Many CRNs may overlap trying to make use of the same spectrum left by a primary network. This behavior is often referred as self-coexistence, there is a requirement for mechanisms to enable coexistence among existing CRNs. 802.22 defines a coexistence beacon protocol (CBP) at the Media Access Control (MAC) layer that address several coexistence needs in a coherent manner [29].

V – THREATS -SOFTWARE DEFINE RADIO AND COGNITIVE RADIO

The purpose of this section is to describe the list of various threats to SDR and CR. The threats will be classified on the basis of the following criteria:

• Security requirements, which are invalidated by the threat.
• Affected SDR or CR function (e.g., spectrum sensing).
• Whether the threat is intentional or unintentional.

A. Software Defined Radio threats

A major security issue which is introduced by the SDR is the consequence of its reconfiguration capability, as described in [30]. SDR terminals must have an ability to download new radio applications or waveforms. Once it is activated, the radio application will alter the radio transmission parameters like frequency, power, and modulation types.

This capability defines two main security issues:-

1) Who guarantees that the downloaded profile or software module (e.g., waveform or radio application) arises from a trusted source and can be activated on the SDR device?
2) Who guarantees that the downloaded profile or software module will act as expected?

We identify the following functionalities in SDR, which can be affected by security threats:-

1) Application management, which includes waveform download and activation.
2) Resource management of computing and processing internal resources of the SDR.
3) Data management to store and retrieve the configuration data used by the waveforms and the operating environment.
4) Internal data transport for the distribution of data among the various modules of the SDR.

A specific type of the data in the SDR is identified by the different types of data that are:-

• User data, which represents the data exchanged and stored in the SDR by the network user.
• Configuration data, which is used by the Software Framework.
• Waveform code, which includes the parameters needed by the specific waveform.

B. Cognitive Radio threats

Communication systems can only change their transmission parameters and use the radio frequency (RF) spectrum bands in the limits, which have been explained by predefined standards and spectrum regulations. These limits are implemented in their hardware and firmware architecture, and they cannot be altered at runtime. A CR may communicate in a wide range of spectrum...
bands and may have the capability to alter its transmission parameters at runtime in response to changes in the sensed radio spectrum environment.

VI- PROTECTION TECHNIQUE- SOFTWARE DEFINE RADIO AND COGNITIVE RADIO

As described in section V, an SDR can be able to the same type of attacks implemented against software computing platforms by downloading and activating malicious software, through the external interfaces of the SDR node. By inserting malicious software, an attacker may implement a variety of security threats:

• Alter or destroy configuration data of the SDR node.
• Implement DoS attacks by overusing computing resources.
• Alter or destroy other software waveforms, the RTOS, or the software framework, even if this would imply access to specific rights and permissions.
• Masquerade as a software waveform.
• Destroy data on the SDR node.
• Unauthorized use of SDR radio services.

To protect against threats, an SDR should be designed with similar mechanisms to the ones adopted to guarantee software assurance in information technology. Software assurance for SDR requires:

• A secure download mechanism, which guarantees the authenticity of the downloaded software. This should be complemented by the components in the SDR terminal to verify the software components.
• A secure execution environment in the SDR terminal to guarantee that only trusted software can be activated and executed.
• Digital signatures could be used to ensure that only authorized software is activated. Trusted computing could also be proposed.
• A module to ensure that spectrum regulations will be validated regardless of the software modules running on the SDR terminal.

VII- SUMMARY

In summary, we can identify the following areas of interest in the near future:

1) Investigate security issues in the integration of SDR/CR technologies with legacy communication systems. In a second step, investigate the evolution of cyber security in next generation wireless IA-enabled ubiquitous communications.
2) Identify realistic operational scenarios to identify which security threats will be more relevant for the end-users.
3) Investigate the integration of a secure download framework integrated with a comprehensive certification process.
4) Investigate the performance impact of protection security solutions in SDR platform to guarantee that real time requirements are still validated.
5) Design tamper-resistance modules to enforce the spectrum regulation policies in the SDR device.
6) Investigate the performance and efficiency of protection techniques based on collaborative spectrum sensing for a realistic deployment.
7) Protection techniques for spectrum management and spectrum sharing functions should be further investigated. Link protection techniques with administrative functions of the network.
8) Further research on protection techniques against threats to the cognitive engine is needed.
9) Support the definition of protection techniques in the current standardization activities for SDR and CR.

VIII- CONCLUSION

The paper gives an overview of the security threats and related protection techniques for SDR and CR technologies. Even if this research field is relatively recent, many contributions have already been proposed and a number of protection techniques are identified. This paper deals with securing Software Define Radio and CRNs and therefore we have presented the function of SDR based Cognitive radio as well as threats and protection technique of Software Define Radio & Cognitive Radio. We have discussed the main research challenges that may change depending on the network management and the type of attacker. We have classified these networks into centralized, partially distributed, and fully distributed; and the attacks according to whether the attacker is part of the CRN or not.

REFERENCES

A Comparative Study of Software Defined Radio and Cognitive Radio Network Technology Security


