Cognitive Radio Network Technology: Security, Architecture and Assessment

Manorma Kaushik, Awanish kumar kaushik, Anubhav kumar, Sweta Kaushik

1, 2, 3 Electronics and Telecommunication Dept
Vishveshwarya Group of Institutions, Dadri, Gr.Noida, India
Manorma_kaushik@yahoo.com
Rajput.anubhav@yahoo.com
awanishkkaushik@gmail.com

4 Department of Master in Computer Application
Institute of Management & Education, Ghaziabad, India
Swetakaushik01@gmail.com

ABSTRACT
Due to the ever-increasing scarcity of spectrum resources, Cognitive radio networks have become an important part of wireless networking system. Such type of networks perform co-operative spectrum which sense to find white spaces and apply various policies to determine when and in which bands they may communicate.

A number of wireless applications have been developing over the last decade. Most of the frequency spectrum has already been certified by Government agencies, like Federal Communications Commission (FCC). Therefore, there is an apparent spectrum scarcity for new wireless services. So the unused spectrum is efficiently utilized by the Cognitive radio for secondary usage without interfering a primary licensed user. In an environment, a primary licensed user can share spectrum occupant’s information with a secondary user to enable dynamic spectrum access.

Cognitive radio is becoming increasingly technology targeting to improve the utilization of the radio electromagnetic spectrum. For performing signal processing, a cognitive radio device uses general purpose computer processors that run radio applications software which enables the device to sense and understand its environment and change its mode of operation based on its observations. Unfortunately, this solution causes new security challenges. Our objective in this paper is to analyze the security issues of recent advancements and architecture of this network and future scope.

Keywords—Cognitive Radio, adaptability, Spectrum sensing.

1. INTRODUCTION
The Cognitive Radio term was first presented by Mitola and Maguire in 1999 [1]. Their original description has received several opinions and result was that the the term Cognitive Radio has become overloaded with many potential meanings [2–4]. From our point of view, Mahmoud defines [4] this most accurately as it clearly reflects the ‘cognitive’ meaning which is related to thinking, reasoning, and remembering. Therefore, we will refer to Cognitive Radio as follows:

Cognitive radio is defined as a smart radio that has an ability to sense the environment, learn from the history, and make more powerful decisions to adjust its communication parameters according to the current status of the environment.

Cognitive radio offers the privilege of intelligent radios that can adapt to their environment. Vast area of research is currently developing various algorithms that allow cognitive radios to operate in a larger variety of different conditions.

Cognitive radios are the latest promising areas in wireless communications that hold promise for better services to many markets, including public safety, military etc. In order to properly, a cognitive radio must be capable of adapting in many directions to adapt the present needs,
changing protocols (set of rules) of the radios without any constraints.

Cognitive radio is an emerging technology for a new spectrum utilization model called opportunistic or distributed spectrum sensing / sharing (OSS/DSS). Cognitive radio can be designed in overlay and underlay fashion. In an overlay fashion, an unlicensed user (also known as secondary users) equipped with cognitive radios function in fallow licensed spectrum bands without causing any disturbances to licensed or primary users [5]; DSS helps to check fallow spectrum bands and maps them into several logical channels [6].

In an underlay fashion, spread spectrum or ultra-wideband techniques along with careful power control [7] are used in such a way that no licensed band receives a strong enough signal to cause interference. A cognitive network has a cognitive process [8] in which current network conditions are accepted, and then plan, decide and act on those conditions.

Since the cognitive radio paradigm imposes human characteristics onto a radio device, a cognitive radio must judge to mitigate the bad manipulations of cognitive radios and cognitive networks into forced behaviors [9].

Due to their intelligent behavior some researches have examined new threats to cognitive radio. Some specific work has been conducted looking at attacks in dynamic spectrum access [10], [11], and was widened to look at a variety of denial of service attacks (DOS) against policy radios [12]. High-level requirements for using cognitive radio sensing and intelligence to address cross-layer security a problem has been examined [13].

Cognitive networks have security necessities at two stages- during environment sensing [14] and during common control channel transactions. A robust common control channel security can save the spread of falsified information which may result due to weak security during environment sensing.

SDR and CR technology which are based on networking systems must validate communication security requirements as Data Confidentiality and Privacy, Availability, Registration, Authentication and Authorization. Standards and regulations are defined for the wireless communication systems, with which SDR and CR devices must interoperate [15-16] is a consequence of the general conformance.

This paper defines the vulnerabilities and potential attacks to this kind of networks covering from the physical to the transport layer of the networks. Attacks to CRNs consist of those common to wireless and ad hoc networks. This paper presents an analysis of some crucial security issues, are important to the design of a strong security model, summary analysis of Cognitive radio security concept and attack type. The paper is structured as follows. Section II presents security requirements, section III presents the various threats present in this technique, in section IV define the various classes of attacks, V define the secure communication link of cognitive radio and applications and conclusions are drawn in section VI.

II. SECURITY REQUIREMENTS

The National Security Agency (NSA) defines Information Assurance IA [17] which is defined as the set of “measuring targeted to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation”.

Security requirements are used for the protection of the data stored or transmitted by the network and also the communication system is able to guarantee the services which are defined by the operational needs.

As mentioned in [18], the definition of the security requirements may be derived considering the concepts of stakeholders, threat and risk.

To eliminate or reduce the security risks, Security actions (protection techniques) are used. Security requirements are an extended version of the network security needs explained by the International Telecommunications Union (ITU) in [19].

The following security requirements are defined:

1) Access to resources: The system should ensure that users will be prevented from accessing to information or resources that they are not authorized to access.

2) Robustness: The system must be able to provide the required communication services in particular service level agreements.
3) **Protection of confidentiality:** The capabilities to ensure the confidentiality of stored and communicated data should be provided by the system.

4) **Protection of system integrity:** The systems must have ability for the integrity of system and its components.

5) **Protection of data integrity:** The system must have ability for the integrity of stored and communicated data.

6) **Compliance to regulatory framework:** The system must be able for the regulations active in that place where the system operates.

7) **Accountability:** The system must be agreed that an entity must accept the responsibility for any of its performed actions. Accountability is used as a synonym of Non-Repudiation.

8) **Verification of identities:** The establishment and verification of the claimed identity of any user is provided by the communication network.

### III. COGNITIVE RADIO THREATS

In this part the components in a generic cognitive radio are described and are explained how they communicate. Then two specific classes of radios are detailed: policy radios and learning radios.

![Cognitive Engine Architecture](image)

**Fig.1. Components within a single cognitive radio**

**Cognitive Engine Architecture:**

A cognitive radio (in Figure 1) consists of four major parts.-First is the software-defined radio (SDR), this is a highly-configurable wireless communications device, has the capability of combining a large number of communications waveforms by composing processing graphs of different radio components [20].

For example, an SDR typically has a front-end allowing it to adjust over different frequency ranges and an amplifier that allows to communicate at many different power levels. Flexibility is possible for many layers which include error correction, data framing, multiplexing, and scheduling.

A wide variety of sensors are also found in SDR. These sensors accept the digitized RF energy and produce a quantitative result. For example, whether or not that channel is occupied, an energy detector can measure the received power at the tuned frequency, to determine Specific waveform detectors. by measuring the autocorrelation and other useful statistics, other sensors can characterize a noise or interference source that can help to design an optimal transceiver. Receiver sensors can determine the current signal-to-noise ratio (SNR), bit and frame error rate.

There are two mechanisms to interact with the knowledge base within the cognitive engine: the reasoning engine and the learning engine. A policy radio has a reasoning engine, while a learning radio has both reasoning and a learning engine.

The reasoning engine is a logical inferencing rules, also called a case-based reasoner. It is a set of actions, the conditions under which those actions are executed, and how those actions affect the state of the knowledge base. The engine proposes the various applications of these rules, searching for a set of actions that will manipulate the state of knowledge base. The combinations of radio configuration values that will maximize some performance metric [20] are selected.

Learning radios include a learning engine therefore they are more flexible. This learning engine has an capability of starting with no preprogrammed policy. For example, a radio can try out different modulation types to see which works in a particular RF environment. Learning radios utilize a variety of AI learning algorithms such as search algorithms, neural networks.

In his dissertation [5], Mitola explains the typical cognition cycle of Observe | Orient | Plan | Decide | Act. If the radio helps to learn, whenever this loop results in a new operating state for the radio, another stage called Learn is injected into the cognition cycle that allows the radio to add its memory information about how the radio transitioned to this new operating state—information that can be used by Plan and Decide in future cognition cycles. In the Mitola’s cognition cycle, the aim of our attacks is to change the Observe stage, and by doing this we can affect the others. Learn has a long-term impact on Act.
These AI features offer an avenue for attackers, as described in the following sections:

A. Policy Radios Threats-
In a policy radio, an attacker spoofs faulty information, causing the radio to select a suboptimal configuration. Radio sensors accept digitized RF and extract useful statistics from it. By understanding how the statistics of radio are calculated, an adversary can change them. Since these statistics operate on RF energy, there is no cryptographic means of securing them, as is frequently done to prevent this communications threats. We call this type of attacks sensory manipulation attacks since they trust on understanding a complex set of logic, and knowing what type of input to provide in order to get the desired output [20].

B. Learning Radios Threats-
Learning radios are the same threats as policy radios. A learning radio makes the attacks more powerful by using all its experiences to develop long-term behavior. For example, an attacker can introduce a jamming signal, forces the radio switches to operate at lower modulation rates whenever a policy radio switches to a faster modulation rate which results in lower link speeds. This will cause link degradation of the attack. However a learning radio forces it to always use lower data rates. After that we describe what effect these attacks can have on a network of cognitive radios.

C. Self-Propagating Behavior-
In such type of an attack, state W on radio R1 will cause behavior that induces state W on radio R2. Once radio R2 is in state W, it can induce that same state on radio R3, and so on. Eventually state W will propagate through all radios in a particular area [20]. Generally, it may not just be a single state W, but it is a series of state transitions W1, WN that introduce the same pattern of state transitions in neighboring radios. A feature of these attacks is that they can spread between non-cooperative radios.

For example, if many devices are trying to share a distributed resource, all devices are traversing the same series of states and executing the same behavior. An adversary may be able to affect this equilibrium such that the asymptotic state is not optimal, and possibly even malicious [20].

IV. CLASSES OF ATTACKS

In this section we describe different scenarios in a cognitive radio network, an attacker can construct by altering knowledge base state on devices. Security is necessary so we define attacks as actions that achieve at least one of the following targets:

• **Unacceptable interference to licensed primary users:** Because of the attack, the communication channel of primary/licensed users of a frequency band becomes unusable that is denial-of-service (DoS) attacks.
• **Missed opportunities for secondary users:** An attacker can prevent secondary users by using available spectrum bands thus reducing channel performance.
• **Access to private data:** By trying to access data in an unauthorized way by the attacker so that as a result the data must be secured by means of cryptographic primitives.
• **Modification of data:** An attacker can try to change the data exchanged between several users for its advantage. Therefore integrity of data must be assured.
• **Injection of false data:** By inducing the false data can make the CRN to perform in an unpredictable way. So the authentication of information sources must be guaranteed.

These attacks to some of the common applications of cognitive radio are related under study:

A. Dynamic Spectrum Access Attacks-
The first type of attack, which was introduced in [10], [11], is called the Primary User Emulation (PUE) attack, and can be effective in dynamic spectrum access (DSA) environments.

In such environments, a primary user has a license to a particular frequency band to use it whenever they wish. Secondary devices can use the available spectrum when they are idle because they need spectrum sensing algorithms to detect when the primary user is active. This attack, coined in [21] as PUEA, is quite realistic by giving the flexibility offered by CRs in terms of transmission parameters. There exist many approaches for spectrum sensing [22]. The most common are energy detection based because of their simplicity because signal is detected by comparing the output of the detector.

B. Objective Function Attacks-
In adaptive radio, under its control the cognitive engine has a large number of radio parameters. The cognitive engine alters these parameters to maximize its multi-goal objective functions. These attacks can be applied to any learning algorithms that utilize objective functions.
In the context of CR, input factors can be frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, authentication type, message integrity code, and frame size [23]. Some possible input parameters could be center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size. The radio may then have three goals: low-power, high-rate, and secure communication. Each of these goals has a different weight depending on the applications.

C. Malicious Behavior Attacks-
In this section an extension of the objective function attacks are discussed where we teach a radio to become unknowingly malicious. Here we find the causes a cognitive radio to become a jammer. Consider a system where a primary user is accessing a channel, secondary users have channel sensing algorithms that can detect primary and secondary users of the channel. The system is used to maximize throughput while minimizing interference. The desired result is a secondary user will only communicate when the primary user is idle. However, if an adversary uses a jamming waveform that cannot be detected by the secondary user’s sensing algorithms, he can decrease when the primary user is idle. By the result, the cognitive radio will learn that when the user is active the only time it can achieve useful communications. This turns the cognitive radio into a jammer.

D. Common control data attack-
In this approach, a dedicated channel is used to exchange the information: (a) between the base station and the secondary users if the CRN is centralized and (b) among secondary users if it is distributed. A malicious user can jam this channel, stopping all transmissions and preventing elements within the CRN from sharing information about spectrum usage [24]. The need of securing the common control data is hence patently obvious. 802.22 Working Group is aware of this threat and has proposed mechanisms to protect such information [25].

E. False feedback-
Where secondary users exchanged sensing information, false feedback from one or a group of malicious users can lead the CRN to take improper actions [26] within a cooperative framework. For example, the CRN can conclude that a given frequency band is occupied by a primary user when actually it is not the case or it could consider it as a vacant band.

F. Lion attack-
Lion attack in [27] as a jamming has a goal to reduce the throughput of Transmission Control Protocol (TCP) by forcing frequency handoffs. The handoff process is a sensing of medium looking for vacant channels and choosing the best one according to some criteria, thus giving the high latencies until the transmission is resumed.

V. COGNITIVE RADIO SECURE COMMUNICATION LINK
As per the IEEE 802.19 standard [28], the essential components of a cognitive radio network are as follows:

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

For the perfect knowledge of the primary users in the licensed spectrum, the secondary users are used to have access to white space database as in Fig. 2, i.e., database containing information of primary users in each and every licensed band. Federal Communications Commissions (FCC) has made spectrum sensing [29] along with access to this white space database. Spectrum sensing is a technique which is used by a CR to detect spectrum holes in the licensed spectrum. Research work which is existed have proposed use of physical layer and medium access control (MAC) layer characteristics of the primary user signal to detect the spectrum holes. The detection process, or 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).

Figure 2- Security in Cognitive Radio Communication explains 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 explained in three stages:

- Step 1: Authenticate a CR,
- Step 2: Authenticate two users in communication, and
- Step 3: Ensure security during the interval of communication between users.

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

**Step 1:** Authenticate a cognitive user
Authentication of a CR can be performed using digital signatures as in [30].

**Step 2:** Authenticate a cognitive user
Authentication of CRs in communication uses the public and private key encryption techniques.

**Step 3:** Secured cognitive communication
The next step is to ensure security in the information being shared after the authentication. All the cognitive users have all the information about the primary user occupied in the desired spectrum. In 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 information, it results that the probability of primary user occupancy in each sub-band is known to each cognitive radio.

**VI. CONCLUSION**
Since the introduction of cognitive radio in 1999 [43], there have been many high-level discussions on proposed capabilities of cognitive radios. This paper consists of securing CRNs and therefore we have presented in it the potential attacks against CRNs. We have also explained the main research challenges that may vary 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 (insider or outsider). The paper has provided an overview of the security threats and related protection techniques for SDR and CR technologies. For the advancement of this field, many contributions have been proposed and a number of protection techniques are defined.

**VII. REFERENCES**


