Computer Communications 36 (2013) 1387–1398

Contents lists available at SciVerse ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

Vulnerabilities in cognitive radio networks: A survey ☆

Shameek Bhattacharjee [a], Shamik Sengupta [b], Mainak Chatterjee [a,*]

[a] Department of Electrical Engineering and Computer Science, University of Central Florida, 4000, Central Florida Blvd, Orlando, FL 32816-2362, United States
[b] Department of Computer Science and Engineering, University of Nevada, Reno 1664 N. Virginia Street, Reno, NV 89557-0208, United States

ARTICLE INFO

Article history:
Received 14 August 2012
Received in revised form 11 June 2013
Accepted 15 June 2013
Available online 24 June 2013

Keywords:
Cognitive radio networks
Vulnerabilities
Security

ABSTRACT

Cognitive radio networks are envisioned to drive the next generation wireless networks that can dynamically optimize spectrum use. However, the deployment of such networks is hindered by the vulnerabilities that these networks are exposed to. Securing communications while exploiting the flexibilities offered by cognitive radios still remains a daunting challenge. In this survey, we put forward the security concerns and the vulnerabilities that threaten to plague the deployment of cognitive radio networks. We classify various types of vulnerabilities and provide an overview of the research challenges. We also discuss the various techniques that have been devised and analyze the research developments accomplished in this area. Finally, we discuss the open research challenges that must be addressed if cognitive radio networks were to become a commercially viable technology.

1. Introduction

Spectrum allocation and management have traditionally followed a 'command-and-control' approach – regulators like the Federal Communications Commission (FCC) allocate spectrum to specific services under restrictive licenses. The restrictions specify the technologies to be used and the services to be provided, thereby constraining the ability to make use of new technologies and the ability to redistribute the spectrum to higher valued services. These limitations have motivated a paradigm shift from static spectrum allocation towards a more 'liberalized' notion of dynamic spectrum management in which non-license holders (i.e., secondaries or secondary networks/users) can 'borrow' idle spectrum from those who hold licensees (i.e., primaries or primary networks/users), without causing harmful interference to the latter– a notion commonly referred to as dynamic spectrum access (DSA) or open spectrum access [1]. It is envisioned that DSA networks enabled with cognitive radio devices [24,35] will bring about radical changes in wireless communications that would opportunistically exploit unused spectrum bands. However, the *open* philosophy of the unmanaged/unlicensed spectrum makes the cognitive radio networks susceptible to events that prevent them from communicating effectively. Just like traditional radios, cognitive radios are not only susceptible to interference but also need spectrum assurance. Unlike traditional radios, cognitive radios constantly monitor the spectrum and intelligently share the spectrum in an opportunistic manner, both in licensed and unlicensed bands. The most important regulatory aspect of these networks is that unlicensed cognitive radios must relinquish their operating channels and move to another available channel as soon as they learn or sense the presence of a licensed user on that channel [11].

As spectrum is made available to unlicensed users, it is expected that all such users will follow the regulatory aspects and adhere to the spectrum sharing and access rules. However, the inherent design of cognitive radios exposes its configuration options to the controlling entity in an effort to make the operational parameters flexible and tunable. As a consequence, configurability and adaptability features open up avenues for manipulation as well. Moreover, problems arise when regulatory constraints are not followed. Also, learning by the cognitive radios is a feature that can be manipulated. A radio can be induced to learn false information by malicious or selfish entities, the effect of which can sometimes propagate to the entire network. It is apparent that the inherent design, flexibility and openness of opportunistic spectrum usage have opened avenues of attacks and made cognitive radio networks susceptible to various genres of vulnerabilities including non-compliance of regulations.

In this paper, we provide a comprehensive overview of the characteristics that make cognitive radio networks vulnerable. The vulnerabilities that arise from the inherent design and protocols of operation are discussed considering different perspectives like objectives, nature of impact, and nature of manipulation. We classify these vulnerabilities based on different criterion and

☆ This study was partially funded by the National Science Foundation, under Award Nos. CCF-0950342 and CNS-1149920.

* Corresponding author.
E-mail addresses: shameek@eecs.ucf.edu (S. Bhattacharjee), ssengupta@unr.edu (S. Sengupta), mainak@eecs.ucf.edu (M. Chatterjee).

0140-3664/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comcom.2013.06.003

understand the rationale behind threats or attacks that have been identified and their subsequent impact. We also provide insight on how vulnerabilities in system design could become potential threats. Subsequently, we discuss the current research developments that deal with ensuring security of cognitive radio networks for various types of attacks. Finally, we present some open research challenges related to trust, security, and protection of cognitive radio networks.

The rest of this survey is organized as follows. Section 2 provides an overview of the cognitive radio architecture and relates how the inherent design principles make them vulnerable to threats. Section 3 provides a classification of various vulnerabilities based on different criterion. Section 4 discusses the context in which each attack/threat is relevant and what their consequences are. In Section 5, the current research developments that have been proposed to mitigate different types of attacks are described and the significance of such developments is analyzed. In Section 6, we put forward some of the open research challenges that must be addressed to make cognitive radio networks commercially viable.

2. Architectural aspects and operational weaknesses

In this section, we present the architectural aspects of cognitive radios and the networks they create. In particular, we focus on the vulnerabilities and threats due to the cognitive functionalities and the architectural aspects of the network that make them prone to different genres of attack.

A typical cognitive radio consists of a sensor, a radio, a knowledge database, a learning engine, and a reasoning engine. A cognitive radio continuously learns from its surroundings and adapts its operational parameters to the statistical variations of incoming radio frequency (RF) stimulus [24]. A cognitive radio selects a set of parameters based on knowledge, experience, cognition, and policies. The parameters chosen optimize some objective function. In the cognitive domain, knowledge or cognizance is obtained from awareness of surroundings, based on input statistics from sensory observations and other network parameters. Optimization of the objective function(s) is governed by the cognitive engine which is shown Fig. 1.

Cognitive radios usually have a programming interface that exposes the configuration options to a controlling entity. The controlling entity could be the service provider that deploys the cognitive radios (base station, access point, etc.) who needs to frequently change the operational parameters– for example, the operating band, access policies, transmission power, and modulation schemes [3,36]. As it is rather impractical to have physical connections with the cognitive radios, the programming of the radios is usually done over-the-air. In the absence of an infrastructure, there might not be any controlling entity and therefore the programming capability could be limited.

2.1. Cognition cycle

The cognition cycle for the cognitive radios is shown in Fig. 2 which primarily consists of three stages: *observe*, *reason and learn*, and *act*. In the observe stage, the radio takes input statistics from the RF environment, updates the knowledge base, and tries to learn the trends with an ultimate aim to optimize a certain objective function during the act stage. It can be noted that, false input statistics in the observe stage can induce incorrect inference, which when shared might propagate throughout the network. As far as learning is concerned, several algorithms based on machine learning, genetic algorithm, artificial intelligence, etc., can be used. With the accumulated knowledge, the radio decides on the operational parameters in such a way that maximizes the objective function at any time instance. At times, different combination of inputs are tried to see if there is a significant change in the objective function. The results are stored in the knowledge base and also fed to the learning algorithms for them to evolve over time.

2.2. Types of cognitive radios

There are three types of cognitive radios: (i) Policy radios, (ii) Procedural cognitive radios, and (iii) Ontological cognitive radios.

Policy radios are governed by a set of rules called the radio's policy [2,6], where they choose a specific subset of rules that is based on factors like the radio's location, the radio environment map, constraints imposed by primary spectrum holder, etc. Spectrum regulators need to ensure that unlicensed cognitive radios have minimal impact over licensed systems, and so there ought to be some implementation of rule based domain knowledge. These may be implemented during the manufacturing, programmed over the air, or configured by a user. The rules might change as the device changes location and falls under the jurisdiction of another primary network. Policy radios generally do not posses learning or reasoning engine. Open questions remain that deal with situations where the policy messages are altered which may lead to regulatory violations.

Procedural cognitive radios are those whose operational adaptation is based on observations by utilizing hard-coded algorithms [37], that specify the different actions necessary for different inputs. Procedural knowledge is summarized as a set of `'if-then-else'` rules. Adaptive actions to be exercised are triggered by certain conditions or observations which may be traced to a pre-defined hard coded function. These are more flexible than the policy radios but not as intelligent as they work in a somewhat deterministic manner taking predictable actions when certain

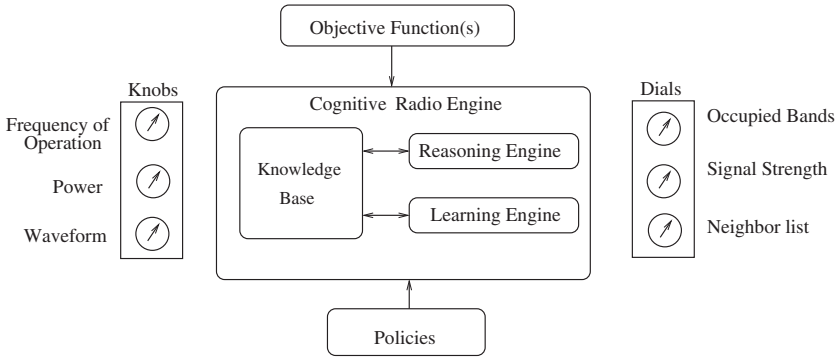

Fig. 1. Architectural overview of cognitive radio.