Contents lists available at ScienceDirect

Computer Networks

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

Survey Paper

A layered approach to cognitive radio network security: A survey

Q1 Deanna Hlavacek *, J. Morris Chang [1]

Q2 College of Electrical and Computer Engineering, Iowa State University, United States

ARTICLE INFO

Article history:
Received 24 September 2013
Received in revised form 6 August 2014
Accepted 1 October 2014
Available online xxxx

Keywords:
Cognitive
Radio
Security
Spectrum
Wireless
Q4 Network

ABSTRACT

Cognitive radios have been identified as a solution to the crowded spectrum issue. With the realization of cognitive radio networks came the recognition that both new and old security threats are relevant. The cognitive radio network is still vulnerable to many of the denial of service, wormhole, routing, and jamming attacks that plague other wireless technologies. In addition, the cognitive radio network is vulnerable to new attacks based on cognitive radio innovations, such as spectrum sharing, spectrum sensing, cognitive capability, and radio reconfigurability. The scope of this survey is to present an overview of security threats and challenges to the cognitive radio network, especially focusing on new solutions from 2012 and the first half of 2013. Included are prior mitigation techniques that are adaptive to the new technology, as well as new mitigation techniques specifically targeted at new cognitive radio vulnerabilities. The threats provided are organized according to the protocol layer at which the attack is targeted.

1. Introduction

It has been estimated that the people of the United States are now outnumbered by their wireless devices. The proliferation of wireless devices such as laptops, notebooks, cellular phones, smart phones, and tablets has caused the frequency spectrum used for transfer of information to become crowded [70]. Also, the expected growth in media-rich consumer applications and wireless data transfer will continue to further crowd the network, making additional spectrum throughput a priority.

Currently in the United States spectrum is allotted to various services in three main categories: licensed, lightly licensed, and unlicensed [1]. Licensed spectrum refers to the portions of the spectrum reserved by each country's equivalent of the Federal Communications Commission (FCC) for specific uses, such as military, public safety, and commercial uses. Lightly licensed spectrum refers to the bands that are generally regulated for licensed users, with regional or other exceptions. In the unlicensed band there are predefined technical rules for the hardware and radio technology intended to mitigate interference between the bands. The spectrum is available for network setup by any person or entity, public or private, to include commercial high speed internet, provided that it does not infringe upon the band's rules [1].

In an effort to provide relief to the users of the overused spectrum, in 2010 the FCC allocated unused spectrum between television channels, or "white spaces" for unlicensed use. In addition, the FCC has proposed setting aside some low band spectrum, and possibly underutilized portions of the military, amateur radio, and paging frequencies, for unlicensed use as long as the primary user experiences no interference. Finally, in early 2013, the FCC

* Corresponding author at: Iowa State University, Ames, IA 50014, United States.

E-mail addresses: deannah@iastate.edu (D. Hlavacek), morris@iastate.edu (J. Morris Chang).

Q3 [1] Tel.: +1 515 294 1097.

http://dx.doi.org/10.1016/j.comnet.2014.10.001
1389-1286/© 2014 Published by Elsevier B.V.

opened a process to allocate more high frequency spectrum for unlicensed use.

In addition to spectrum overcrowding, one of the major challenges for the wireless medium is security. The WiFi brand was adopted in 1999 based on the 802.11 standard. It was immediately realized that using the electromagnetic wave as the propagation medium made physical security of the transmitted data an impossibility. A conversation made of electromagnetic signals can be intercepted, jammed, or injected with extraneous bits. These actions can cause the release of private information, the inability to send and receive information, or the receipt of false or unreadable data.

As with other wireless communications, the cognitive radio technology based on the 802.22 standard must enforce the security triad of confidentiality, integrity, and availability (CIA). The cognitive radio is subject to many of the same types of attacks that plague other cellular and wireless communication systems. In addition, due to the cognitive radio's ability to self-organize a network and establish routing similar to wireless sensor networks (WSNs), the cognitive radio network (CRN) is also vulnerable to attacks originally designed for WSNs. Finally, the abilities of the CRN to sense the environment, adjust spectrum usage parameters, collaborate with neighbors, and learn provide new avenues for attack.

Because cognitive radio is in its infancy, there are many opportunities for research into the security issues to which the new technology is vulnerable. Such research can drive the creation of a more secure product. The papers [9,55,69] provide a general overview of the cognitive radio network model with a broad description of secure model considerations. The authors of [54] provide a very extensive overview of all cognitive radio network issues, with an in depth look at the security issues specific to the new CRN vulnerabilities.

The papers [41,91] each provide a high level view of the legacy and newer threats that can be applied to the cognitive network. The authors of [6,92] both take a broad stroke at listing and describing threats specific to the cognitive radio. In addition, the paper [6] adds a focus on the threats specific to the policy controlled cognitive radio. An in-depth look at the primary user emulation attack and mitigation is presented by the authors of [84,92]. The paper [74] analyzes vulnerabilities of existing spectrum sensing and access protocols under stochastic channels in the presence of jamming attacks. The authors of [78] concentrate on the vulnerabilities of the physical layer.

Comprehensive, security focused studies for the cognitive radio network were presented by [7,27,63,76]. The paper [76] takes the traditional approach of describing the possible attacks on a CRN. The authors of [7] categorize and analyze the threat vectors (as compared to attacks) and provides design considerations to alleviate the threats. A discussion on security evaluation and certification is included. Rather than analyzing the threats or attacks to the cognitive radio, the paper [27] analyzes the 2010 and earlier solutions presented to mitigate CRN security issues.

The paper [63] takes a layered approach in its study of cognitive radio network security. Four layers are presented: security applications, security strategies, security infrastructure, and security primitives. Threats are also presented in categories: learning, hidden node, policy, parameter, and sensing.

The security professional must be properly prepared for the battle that will ensue as the cognitive radio network comes into use. To that end, the purpose of this paper is to provide a survey of security issues related to the cognitive radio network. Potential attacks will be described, and proposed mitigation techniques will be explored. The attacks in the survey are presented according to the targeted protocol layer. Emphasis has been placed on presenting solutions proposed in 2012 and early 2013, when available. The remainder of the paper is organized as follows: Section 2 describes the general concepts and security considerations of the cognitive radio. Starting at Section 3 the paper presents attacks and mitigation techniques based on communication layer protocols. Sections 3–7 present the Physical layer, Data link layer, Network layer, Transport layer, and Application layer, respectively. Section 8 presents the Cross-layer attacks. Section 9 provides a conclusion. Table 1 will provide snapshots of the attacks presented by layer.

2. Cognitive radio

The cognitive radio is based on a software defined radio with adjustable operational parameters [2]. The software allows the radio to tune to different frequencies, power levels, and modulation schemes to establish or maintain a communication link. The hardware consists of an antenna, a radio frequency conversion module, a modem, and other modules [57]. The best configuration for the radio is determined by optimizing an objective function that considers such factors as interference and noise, traffic demand, mobility levels, and location.

In addition to the variable parameters mentioned above, the cognitive radio network is further adaptable to changing situations with its ability to operate successfully in collaborative (cooperative) or uncooperative networks. Generally, the throughput of the collaborative network will be higher than that of the uncooperative network due to the ability of the cooperating radios to share the frequency to which they will hop. However, when the network is under certain types of attacks, or in certain environmental situations, the uncooperative network configuration may be optimal. We must therefore analyze attacks and mitigation techniques for both scenarios.

It is generally agreed that the cognitive radio must provide the following functions: spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility. Spectrum sensing is required for the cognitive radio to sense the spectrum for the presence of the primary user or other traffic. Through spectrum management the radio is able to utilize the available spectrum efficiently without interfering with the primary user. The protocols established in the IEEE 802.22 standard govern the ability of the radio to share the spectrum with the primary user and other secondary users. The radio is able to vacate a spectrum when the primary user is indicated as present while continuing communication with the network due