Computer Networks 115 (2017) 130–138

Contents lists available at ScienceDirect

Computer Networks

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

A framework for resilient and secure spectrum sensing on cognitive radio networks

Julio Soto, Michele Nogueira*

Department of Informatics, Federal University of Paraná, Curitiba-PR, Brazil

ARTICLE INFO

Article history:
Available online 22 January 2017

Keywords:
Cooperative spectrum sensing
Cognitive radio networks
Security management
Framework
Adaptation

ABSTRACT

Cognitive radio networks have been envisaged to improve efficiency in accessing the frequency spectrum. However, these networks are prone to different kind of attacks and failures that can compromise the security and performance of licensed and unlicensed users. The main contribution of this work lies in a framework for security and resilience in cognitive radio networks. As a showcase, this framework is applied to spectrum sensing functionality in order to assist its operation even in face to failures and attacks, such as primary user emulation ones. Differently from other proposals founded on specific and permanent device features, our framework provides *flexibility* and *adaptation* for detection and mitigation mechanisms considering best-efforts or real-time applications. Simulation results based on real traces provide evidences about the improvements achieved by our framework on spectrum sensing, even under primary user emulation attacks.

1. Introduction

Advances toward opportunistic spectrum access have attracted the attention of scientific communities and industry in order to have an efficient way to use the radio frequency spectrum. Cognitive radio (CR) has been envisioned as a key technology to provide high bandwidth for fixed and mobile users through dynamic spectrum access techniques [1]. This technology allows unlicensed secondary users (SUs) to exploit idle licensed frequency bands for improving communication between pairs of users on a cognitive radio network (CRN) [2]. Cognitive radios can autonomously adjust their parameters and modify their behavior based on their operational electromagnetic environment.

Spectrum sensing is the most important phase in the cognitive cycle [3,4]. It provides to the radio the ability to measure, sense, learn, and be aware of the parameters related to channel characteristics. Furthermore, it is able to detect temporarily unused frequencies, often referred to as spectrum holes or *white spaces*, without causing interference to the licensed or primary user activities [4]. The accuracy on detecting spectrum holes determines the efficiency of the three successive phases on the cognitive cycle, as spectrum decision, sharing and mobility, since all their functionalities will be based on spectrum holes information from spectrum sensing. Imprecisions in white space detection can result in inaccurate decisions by SUs, increasing the number of collisions in sharing frequencies, and also compromising cognitive radio and primary networks performance due to low quality in sensing primary user activities.

Despite of cognitive radio advantages, this technology is still constrained by challenges and issues in the spectrum sensing phase. First, centralized or decentralized spectrum sensing techniques are prone to unexpected faults in hardware and software [4]. Second, their operation allows misbehaving secondary users to benefit from CR reconfigurability abilities to manipulate their radio parameter values or inject false data in the network, taking advantage on frequency spectrum opportunities or compromising legitimate secondary users performance. Third, the complexity of the envisioned multi-dimensional spectrum sensing approach can increase the probability of CRNs be harmed, since multiple dimensions are employed to obtain the spectrum usage characteristics, such as time, space, frequency, and code, making control difficult [4]. Further, cognitive radio characteristics make CRN prone to new security weaknesses, such as primary user emulation (PUE) attacks, in which misbehaving secondary users pretend primary users behavior in order to have priority in accessing spectrum holes.

Security has received increasing attention in cognitive radio technology [5–7]. Recently, protocols, architectures and standards have been created considering security aspects [8–10]. IEEE 802.22 standard [10], for instance, provides a security sub-layer designed

DOI of original article: 10.1016/j.comnet.2015.01.011
* Corresponding author.
E-mail addresses: jchsoto@inf.ufpr.br (J. Soto), michele@inf.ufpr.br (M. Nogueira).

http://dx.doi.org/10.1016/j.comnet.2017.01.012
1389-1286/

in order to achieve confidentiality, authentication and data integrity by cryptographic transformations in link-layer data units. However, those proposals use conventional security techniques, such as cryptography, intrusion detection system and authentication, that are not enough to prevent spectrum sensing against attacks and intrusions [5]. Preventive security mechanisms, as cryptography, provide confidentiality, integrity and authentication, but they are inefficient against overload, interception, manipulation or impersonation attacks, such as Denial of Services (DoS), PUE attacks and jamming. Reactive security mechanisms, as intrusion detection systems (IDS), are based on network behavior analysis, or previously known attack and intrusion patterns. Since new communication technologies are more dynamic and adaptive, attacks are also smarter, easily bypassing common security mechanisms [5,11].

In face to these constraints, new designs for resilience and security in spectrum sensing must be provided considering cognitive radio characteristics and being more flexible to cope with attacks mutations. Hence, this work presents the Reliable and secure cOgnitive radiO networK (ROOK) framework for managing security mechanisms in order to achieve resilience and security against attacks and intrusions on cognitive radio networks. Different from previous works [6,7], this one presents a holistic approach that seeks to not only detect PUE attacks, but also to provide resilience and security against a broader range of attacks and intrusions on cognitive radio networks. As a showcase, it is applied to spectrum sensing, intending to show improvements resulted from the flexibility capability and from the multiple dimensional spectrum sensing on the detection and mitigation of PUE attacks. In the showcase, the proposed framework is instantiated to employ the Normalized Weighted Additive Utility Function (NWAUF), a multi-criteria analysis technique to estimate preliminary probabilities about the presence of attacks in the network; and to apply the non-parametric Bayesian inference to calculate the final probability of existing attacks in the network. Based on real traces, simulation results from two different case studies show the improvements achieved by our approach in terms of attacks detection and adaptation to network conditions.

This article proceeds as follow. In Section 2, we overview related works, and the challenges related to resilience and security in CRNs. In Section 3, we detail the proposed framework. In Section 4, we showcase the framework in the context of spectrum sensing. In Sections 5 and 6, we present simulation setup and results for the framework instantiation. Finally, in Section 7, we present our conclusions and highlight future works.

2. Motivation

2.1. Related work

From the literature, different protocols, architectures and standards have been created considering security aspects [7–10]. In general, those works focus on specific attacks and defense mechanisms, being the most prominent the detection of PUE attacks. Chen and Park, for instance, introduced PUE attacks in the literature [12,13]. In their works, authors discussed how the CR technology is vulnerable to this attack and proposed a “transmitter verification procedure” to distinguish between incumbent signals from emulated signals. The proposed scheme defines PUs as UHF TV towers with known locations, and that transmission power of PUs is several orders of magnitude higher than the transmission power of attackers. Thus, they use the received signal strength to infer distance and, based on this, they analyze the presence of a PUEA in the CR network.

In [14], Jin et al. argue that location-based solutions like the ones proposed in [12,13,15] usually require a dedicated wireless sensor network to assist the localization of transmitters. Thus, they design a different scheme that employ the received signal strength as decision criterion. In turn, Li and Han [16] also propose alternatives to the location-based criterion. They handle scenarios in which the power of a PU is not several order of magnitudes higher than the attacker’s (e.g. mobile attacker), which leads location-base criterion to fail in the PUEA detection. Then, they design a zero-sum game scheme that uses the occupancy probability of multiple different channels to establish a Nash equilibrium. Such probabilities are estimated according to criteria based on received power or cyclostationary features. In [17], energy detection and location verification are employed to mitigate the performance degradation of a CR network under a PUE attack. The authors employ a two-level database-assisted detection approach and admission control techniques to achieve their goals.

In [18], authors advances the literature employing radio-specific signals as criteria to detect PUE attacks, such as amplitude, frequency and bandwidth. Authors argue that differently from previous employed criteria, as location, power transmission and others, the values of the radio-specific criteria are features that cannot be easily changed on the hardware post-production. Authors employed nonparametric Bayesian classification in the definition of the DECLOAK proposed method. Despite of presenting satisfactory results in PUE attacks detection, DECLOAK cannot be easily adapted to attacks behavior mutations without the necessity to redesign it.

Chen et al. [19] are the firsts to discuss the PUEA in the context of mobile CR networks where the PUs are wireless microphones. They emphasize that the detection criteria employed by prior works are not meaningful for that type of networks because the properties of the microphones-based networks i.e., low transmission power and mobility. Hence, they propose a new method to detect PUEAs in which the criteria is designed to take into account not only RF signals, but also acoustic information. In [20], authors also addressed the PUE attacks detection in mobile cognitive ad hoc networks. However, the employ Channel-tap power as fingerprints to detection.

The state of art in the field of PUEA detection evolved from some network architectural aspects (i.e. from non-cooperative centralized approaches e.g. [12–14,16] to cooperative and/or distributed ones (e.g. [18,21–24]). In [7], the authors presented an approach mainly focused on the perspective to provide flexibility to the criteria employed to detect PUE attacks in cognitive radio ad hoc networks. The main idea consisted in how easily a solution could adapt the criterion employed to the PUEA detection.

Despite of those efforts, solutions still require the capability to cope with the new dynamics resulted from advances in communication technologies. As communication technology evolve, attacks also advance easily bypassing common security mechanisms [5,11]. The simple use of conventional security techniques, such as cryptography, intrusion detection system and authentication, is not enough to prevent spectrum sensing against attacks and intrusions [5]. In general, they are inefficient against overload, interception, manipulation or impersonation attacks, such as Denial of Services (DoS), PUE attacks and jamming. Hence, new designs for resilience and security in spectrum sensing must be provided considering cognitive radio characteristics and being more flexible to handle attack mutations.

2.2. Resilience and security challenges in spectrum sensing

Wireless communication networks, such as CRN, have evolved tremendously over the past several years, supporting services for users daily activities and becoming essential for them. As this evolution is still progressing, users requirements and expectations increase in terms of performance and dependability due to the high