Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 73 (2015) 199 – 208

Procedia Computer Science

The International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Cognitive Radio Jamming Mitigation using Markov Decision Process and Reinforcement Learning

Feten Slimeni[a,*], Bart Scheers[b], Zied Chtourou[a], Vincent Le Nir[b], Rabah Attia[c]

[a] *VRIT Lab - Military Academy of Tunisia, Nabeul 8000, Tunisia*
[b] *CISS Departement - Royal Military Academy (RMA), Brussels 1000, Belgium*
[c] *SERCOM Lab - EPT University of Carthage, Marsa 2078, Tunisia*

Abstract

The Cognitive radio technology is a promising solution to the imbalance between scarcity and under utilization of the spectrum. However, this technology is susceptible to both classical and advanced jamming attacks which can prevent it from the efficient exploitation of the free frequency bands. In this paper, we explain how a cognitive radio can exploit its ability of dynamic spectrum access and its learning capabilities to avoid jammed channels. We start by the definition of jamming attacks in cognitive radio networks and we give a review of its potential countermeasures. Then, we model the cognitive radio behavior in the suspicious environment as a markov decision process. To solve this optimization problem, we implement the Q-learning algorithm in order to learn the jammer strategy and to pro-actively avoid jammed channels. We present the limits of this algorithm in cognitive radio context and we propose a modified version to speed up learning a safe strategy. The effectiveness of this modified algorithm is evaluated by simulations and compared to the original Q-learning algorithm.

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)

Keywords: Cognitive radio network, jamming attack, Q-learning algorithm

1. Introduction

Cognitive Radio (CR) technology is recognized as an intelligent radio that is able of learning and reconfigurability in order to automatically detect available channels in wireless spectrum and perform a real time adaptation to the environment modifications [1,2]. Its ability of dynamic spectrum management makes it a promising solution to overcome the problems of scarcity and inefficient utilization of the radio spectrum, but makes it more susceptible to be jammed. Furthermore, cognitive radio networks (CRNs) are characterized by dynamic spectrum access (DSA) and by mainly distributed architectures which make it difficult to implement effective jamming countermeasures.The jammers can be classified according to the following criteria:

- Spot/Sweep/Barrage jamming
  Spot jamming consists in attacking a specific frequency, while a sweep jammer will sweep across an available frequency band. A barrage jammer will jam a range of frequencies at once.
- Single/Collaborative jamming

Peer-review under responsibility of organizing committee of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT 2015)
doi:10.1016/j.procs.2015.12.013

The jamming attack can be done by a single jammer or in a coordinated way between several jammers to gain more knowledge about the network and to efficiently reduce the throughput of the cognitive users.

- Constant/Random jamming
  The jammer can either send jamming signals continuously on a specific channel or alternate between jamming and sleeping.
- Deceptive/Reactive jamming
  A deceptive jammer continuously transmits signals in order to imitate a legitimate or primary user. A reactive jammer transmits only when it detects busy channel to cause collisions.

In this paper, we start by a review of the common anti-jamming techniques in CRNs. Then, we model the CR behavior in the suspicious environment as a markov decision process (MDP). To solve this optimization problem, we explain in section 4 how the Q-learning can be used to learn the jamming strategy and to pro-actively avoid the jammed frequencies. However, using the standard version of this algorithm present several limits in CRNs, so we present a modified version making the learning process safer and faster. We evaluate the effectiveness of this modified algorithm in the presence of different jamming strategies. The simulation results are compared to the original Q-learning algorithm applied to the same scenarios.

2. Review of CR jamming attack countermeasures

The jamming attack has been widely exploited as strategic maneuver in military wireless communications. This problem has been intensively researched for traditional wireless networks but it is still a challenging issue in CRNs.

We present in this section an overview of the proposed anti-jamming techniques in CRNs. We start by the traditional anti-jamming solutions used in wireless networks, which consist in spread spectrum techniques by the use of either frequency hopping (FH) or direct-sequence spread spectrum (DS-SS) methods[3]. These solutions can be enhanced to mitigate the jamming attack in CRNs. Then, we present another class of anti-jamming techniques which aim to correct the already jammed data during transmission. There are solutions to deceive the jammers instead of escaping from it or repairing its effect on the transmitted data. And finally, we present how game theory is used in related papers to model the jamming attack in CRNs and to find optimal anti-jamming strategies.

2.1. Frequency hopping

The CR is characterized by its ability of dynamic spectrum access to use the spectrum in opportunistic way. This ability can be exploited to overcome jamming attacks since the CR can change its operating frequency to avoid the jammers. However, the exploitation of frequency hopping in CRN anti-jamming approaches present a trade-off between the resource consumption every time to change the jammed frequency and the jamming impact if the CR still using the same frequency even jammed.

Recently, diverse CRN frequency hopping defense strategies, were analyzed.[4] presented proactive or impetuous hopping (selecting a new set of frequencies at every slot, irrespective of the jamming) and reactive or conservative hopping (unjammed users keep the same frequencies for the next slot, while the jammed users choose a set of new unused frequencies that exclude the jammed ones). The authors proposed a multi-tier proxy based cooperative defense strategy, in which users form tiers to exploit the temporal and spatial diversity to avoid jamming.

2.2. Direct-sequence spread spectrum (DS-SS)

This spread spectrum technique consists in spreading the signal over several pieces of non-overlapping channels. It can be exploited as an anti-jamming technique because the jammer will have to choose either to jam a large number of channels with negligible jamming effect in each one or to jam only few channels with important effect. The authors in[5], proposed an uncoordinated spread spectrum technique that enables anti-jamming broadcast communication without predefined shared secrets. They aimed to improve the common spread spectrum which depends on secret pairwise or group keys shared between the sender and the receivers before the communication, to adapt it for critical applications such as emergency alert broadcasts and military communications.