Applied Soft Computing xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Applied Soft Computing

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

Review article

Application of reinforcement learning for security enhancement in cognitive radio networks

Q1 Mee Hong Ling[a,*], Kok-Lim Alvin Yau[a], Junaid Qadir[b], Geong Sen Poh[c], Qiang Ni[d]

[a] Department of Computing and Information Systems, Sunway University, No. 5 Jalan Universiti, Bandar Sunway, 46150 Petaling Jaya, Selangor, Malaysia
[b] Electrical Engineering Department, School of Electrical Engineering & Computer Science, National University of Science and Technology, Sector H12, Islamabad, Pakistan
[c] University Malaysia of Computer Science & Engineering (UniMy), Jalan Alamanda 2, Presint 16, 62150 Putrajaya, Malaysia
[d] School of Computing & Communications, Lancaster University, Lancashire LA1 4YW, United Kingdom

ARTICLE INFO

Article history:
Received 10 March 2015
Received in revised form 21 July 2015
Accepted 1 September 2015
Available online xxx

Keywords:
Reinforcement learning
Trust
Reputation
Security
Cognitive radio networks

ABSTRACT

Cognitive radio network (CRN) enables unlicensed users (or secondary users, SUs) to sense for and opportunistically operate in underutilized licensed channels, which are owned by the licensed users (or primary users, PUs). Cognitive radio network (CRN) has been regarded as the next-generation wireless network centered on the application of artificial intelligence, which helps the SUs to learn about, as well as to adaptively and dynamically reconfigure its operating parameters, including the sensing and transmission channels, for network performance enhancement. This motivates the use of artificial intelligence to enhance security schemes for CRNs. Provisioning security in CRNs is challenging since existing techniques, such as entity authentication, are not feasible in the dynamic environment that CRN presents since they require pre-registration. In addition these techniques cannot prevent an authenticated node from acting maliciously. In this article, we advocate the use of reinforcement learning (RL) to achieve optimal or near-optimal solutions for security enhancement through the detection of various malicious nodes and their attacks in CRNs. RL, which is an artificial intelligence technique, has the ability to learn new attacks and to detect previously learned ones. RL has been perceived as a promising approach to enhance the overall security aspect of CRNs. RL, which has been applied to address the dynamic aspect of security schemes in other wireless networks, such as wireless sensor networks and wireless mesh networks can be leveraged to design security schemes in CRNs. We believe that these RL solutions will complement and enhance existing security solutions applied to CRN To the best of our knowledge, this is the first survey article that focuses on the use of RL-based techniques for security enhancement in CRNs.

Contents

Q2 * Corresponding author. Tel.: +60 37491 8622x7135; fax: +60 35635 8633.
E-mail addresses: mhling@sunway.edu.my (M.H. Ling), koklimy@sunway.edu.my (K.-L.A. Yau), junaid.qadir@seecs.edu.pk (J. Qadir), poh@unimy.edu.my (G.S. Poh), q.ni@lancs.ac.uk (Q. Ni).

http://dx.doi.org/10.1016/j.asoc.2015.09.017
1568-4946/

1. Introduction

Q4

Cognitive radio (CR) [1,2] is the next-generation wireless communication system that promises to address the artificial spectrum scarcity issue resulting from the traditional static spectrum allocation policy through dynamic spectrum access. With dynamic spectrum access, unlicensed users, or secondary users (SUs), can opportunistically exploit underutilized spectrum owned by the licensed users or primary users (PUs). Hence, CRs can improve the overall spectrum utilization by improving bandwidth availability at SUs. To achieve these functions, artificial intelligence (AI) techniques have been adopted in CR so that the SUs can sense, learn, and adapt to the dynamic network conditions, in which the PUs' and malicious users' activities appear and reappear. Cognitive radio networks (CRNs) can operate in both centralized and distributed settings: a centralized CRN consists of a SU base station (or access point) that communicates with SU nodes while a distributed network consists of SU nodes that communicate with each other in an ad-hoc manner.

CRNs rely on cooperation for much of their functionality. While such a reliance on cooperative algorithms can make CRNs more efficient, this also opens CRNs up to numerous security vulnerabilities. One of the important requirements of CRNs is that SUs must minimize harmful interference to PUs. This requires SUs to collaborate amongst themselves to perform channel sensing and make accurate final decision on the availability of a channel. However, such collaboration among SUs may pose a security challenge to the SUs' trustworthiness. For instance, in collaborative channel sensing, the legitimate (or honest) SUs depend highly on the dynamic allocation of a common control channel (CCC), which is used for the exchange of control messages during normal operations. However, the collaborating SUs may be malicious, and they may intentionally provide false sensing outcomes to interfere with the PUs or the other SUs, as well as to launch jamming attacks on the CCC, which adversely impacts performance and causes transmissions to come to a halt [3]. Hence, such SUs need to be detected and ignored in collaboration. The aforementioned discussion highlights that CRNs are susceptible to various attacks, such as channel jamming, eavesdropping or packets alteration. Further details on CRNs vulnerabilities, attacks and security threats can be found in detailed survey articles on this topic [4–6].

The main security challenge in a CRN is that it operates in a dynamic set of licensed and unlicensed channels (in contrast to traditional wireless networks that typically operate with a fixed set of limited channels). In addition, the dynamic nature of the activities of PUs and malicious nodes requires SUs to change their operating channels from time to time: hence, longer-term knowledge is necessary so that SUs do not oscillate or constantly switch their actions within a short period of time. With this inherent characteristic, a mechanism to manage and learn from the ever-changing environment is needed to tackle the security challenge.

Reinforcement learning (RL) is an artificial intelligence (AI) approach that helps a decision maker (or agent) to learn the optimal action through repeated interaction with the operating environment [7]. RL is an unsupervised and intelligent approach that enables an agent to observe and learn about the static or dynamic operating environment in the absence of guidance, feedback or the expected response from supervisors (or external critics), and subsequently make decisions on action selection in order to achieve optimal or near-optimal system performance. RL has been adopted in the literature [8–16] because it does not require prior knowledge of channel availability and it is highly adaptive to the dynamicity

Please cite this article in press as: M.H. Ling, et al., Application of reinforcement learning for security enhancement in cognitive radio networks, Appl. Soft Comput. J. (2015), http://dx.doi.org/10.1016/j.asoc.2015.09.017