An Adaptive Trust-Stackelberg Game Model for Security and Energy Efficiency in Dynamic Cognitive Radio Networks

He Fang, Li Xu, Jie Li, Kim-Kwang Raymond Choo

PII: S0140-3664(16)30628-4
DOI: 10.1016/j.comcom.2016.11.012
Reference: COMCOM 5415

To appear in: *Computer Communications*

Received date: 22 February 2016
Revised date: 28 October 2016
Accepted date: 29 November 2016

Please cite this article as: He Fang, Li Xu, Jie Li, Kim-Kwang Raymond Choo, An Adaptive Trust-Stackelberg Game Model for Security and Energy Efficiency in Dynamic Cognitive Radio Networks, *Computer Communications* (2016), doi: 10.1016/j.comcom.2016.11.012

An Adaptive Trust-Stackelberg Game Model for Security and Energy Efficiency in Dynamic Cognitive Radio Networks

He Fang[a], Li Xu[a,*], Jie Li[b], Kim-Kwang Raymond Choo[c]

[a] *Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China.*
[b] *Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba Science City, Ibaraki 305-8573, Japan.*
[c] *Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249-0631, USA.*

Abstract

Due to the potential of cooperative cognitive radio networks (CCRNs) in addressing the spectrum scarcity problem in wireless communication networks, CCRN has become a subject of active research. For example, security and energy efficiency are two salient areas of research in CCRNs. In this paper, we propose a novel adaptive trust-Stackelberg game model designed to (a) improve the energy efficiency and (b) defend against insider attacks in CCRNs. More specifically, the distributed learning algorithm (DLA) for the relays in our model, inspired by the stochastic learning automata, allows the system to achieve Stackelberg equilibrium in the proposed game; and the trust evolution based on evolutionary stable strategy algorithm (TEEA) allows the primary user to defend against insider attacks efficiently and adaptively adjust the trust evolution in dynamic CCRNs. We demonstrate the utility of the proposed model comparing with other models using a numerical investigation. The numerical results show that the proposed model can improve the performance in energy efficiency and defending against insider attacks with an appropriate cooperation between primary users and relays.

*Corresponding author
URL: xuli@fjnu.edu.cn (Li Xu)