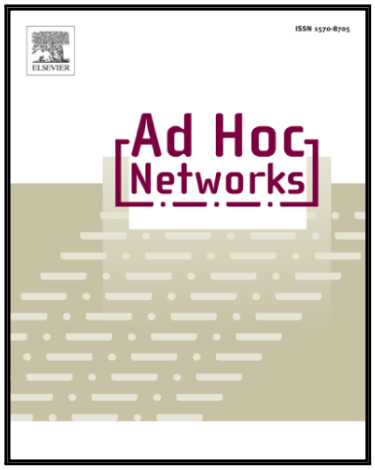
Journal Pre-proof



Intelligent Jamming-aware Routing in Multi-hop IoT-based Opportunistic Cognitive Radio Networks

Haythem Bany Salameh, Safa Otoum, Moayad Aloqaily, Rawan Derbas, Ismaeel Al Ridhawi, Yaser Jararweh

PII: S1570-8705(19)30636-5
DOI: https://doi.org/10.1016/j.adhoc.2019.102035
Reference: ADHOC 102035

To appear in: *Ad Hoc Networks*

Received date: 11 July 2019
Revised date: 17 October 2019
Accepted date: 30 October 2019

Please cite this article as: Haythem Bany Salameh, Safa Otoum, Moayad Aloqaily, Rawan Derbas, Ismaeel Al Ridhawi, Yaser Jararweh, Intelligent Jamming-aware Routing in Multi-hop IoT-based Opportunistic Cognitive Radio Networks, *Ad Hoc Networks* (2019), doi: https://doi.org/10.1016/j.adhoc.2019.102035

Intelligent Jamming-aware Routing in Multi-hop IoT-based Opportunistic Cognitive Radio Networks

Haythem Bany Salameh[a,b], Safa Otoum[c], Moayad Aloqaily[a,d], Rawan Derbas[b], Ismaeel Al Ridhawi[e], and Yaser Jararweh[f]

[a] *Al Ain University of Science and Technology, Al Ain, UAE*
[b] *Yarmouk University, Jordan*
[c] *University of Ottawa, Ottawa, ON, Canada*
[d] *xAnalytics, Ottawa, ON, Canada*
[e] *Kuwait College of Science and Technology (KCST), Kuwait*
[f] *Jordan University of Science and Technology (JUST), Irbid, Jordan.*

Abstract

Cognitive Radio Networks (CRNs) have emerged as a promising next-generation network technology that solves the spectrum scarcity issue and improves spectrum utilization. It is designed to help grant access for unlicensed users and utilize the maximum available licensed bandwidth. Moreover, the Internet of Things (IoT) has brought a significant promise to a multitude of applications and services allowing for anytime and anywhere connectivity. The coexistence of IoT and CRN has enabled a broad range of solutions to be available for users in an efficient and somewhat secure manner. But, with today's resource consuming and time-sensitive IoT applications, the lack of communication security proves to be a challenge. CRNs are prone to more attacks and have much more risks than traditional wireless networks. This paper introduces a security-aware routing protocol that considers jamming attacks which interrupt cognitive radio transmissions. The proposed protocol assigns the most secure channel for each hop within an IoT source-destination pair in accordance to an optimization problem. Moreover, since CRNs are more vulnerable to threats, an Ensemble-based Jamming Behaviour Detection and Identification (E-JBDI) technique is proposed as a second line of defence. It is used to identify the behavior anomaly of jamming attack. Extensive simulations are conducted to showcase the effectiveness of the proposed routing protocol in comparison to other relatively similar state-of-the-art solutions. Results show network performance improvements against increased numbers of proactive jamming attacks. Moreover, results also show the effectiveness of E-JBDI in terms of accuracy, detection and precision-recall rates with values of ≈ 1.

Keywords: Security, Artificial Intelligence, Machine Learning, Jamming Attack, Jamming Detection, IoT, Cognitive Radio Networks.

1. Introduction

Cognitive radio networks (CRNs) allow unlicensed Cognitive Radio (CR) devices the use of underutilized spectrum in licensed frequency bands, thus, improving spectrum utilization and

Email addresses: haythem.banysalameh@aau.ac.ae (Haythem Bany Salameh), Safa.Otoum@uOttawa.ca (Safa Otoum), maloqaily@ieee.org (Moayad Aloqaily), Rderbas@yu.edu.jo (Rawan Derbas), i.alridhawi@kcst.edu.kw (Ismaeel Al Ridhawi), yijararweh@just.edu.jo (and Yaser Jararweh)