Chapter 5
Selective Cooperative Jamming Based Relay Selection and Blowfish Encryption for Enhancing Channel and Data Security in CRAHN Routing

Hesham Mohammed Ali Abdullah
Hindusthan College of Arts & Science, India & Bharathiar University, India

A.V. Senthil Kumar
Hindusthan College of Arts & Science, India & Bharathiar University, India

ABSTRACT

The problems of security and secret communication for the secondary users in the cognitive radio ad hoc networks (CRAHNs) have been extensively researched. Most routing protocols in CRAHNs, though providing efficient routing, do not produce satisfactory secrecy rate and security. One such model is spectrum-map-empowered opportunistic routing (SMOR) which has been the motivation behind this research contribution. A better and secured routing algorithm is developed in this chapter by modifying and enhancing the SMOR model. As the relay selection enables the secrecy in communication between the users, selective cooperative jamming (SCJ) based relay selection is utilized in the proposed model. This approach generates weighted jamming signals in selected relays to create high interference in the communication direction other than the legal users and confuses the eavesdroppers. For secured data transmission, data encryption processes are carried out using a blowfish encryption algorithm. This further strengthens the security in communication between users on the same frequency and also helps in avoiding the eavesdropping attacks. The performance of this proposed model named as SCJ with Blowfish Modified SMOR (SCJB-M-SMOR) has been evaluated and the comparison results showed it has better secrecy rate and secrecy outage probability.

DOI: 10.4018/978-1-5225-6023-4.ch005

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

1. INTRODUCTION

Cognitive radio (CR) is an opportunistic communication technology designed to utilize the maximum available licensed bandwidth for unlicensed users (Haykin, 2005). As wireless communication devices have been massively boundless, unnecessary spectrum requests and the need to better use the accessible spectrum have been faced. In conventional spectrum management, a large portion of the spectrum is distributed to authorized users for selective usage. CR technology is completed in two stages (Fette, 2009). Initially, it scans for accessible spectrum bands by a spectrum-detecting approach for unlicensed secondary users (SUs). At the point when the authorized primary user (PU) isn't utilizing the spectrum bands, they are viewed as accessible. Second, accessible channels will be assigned to unlicensed SUs by unique flag get to conduct. At whatever point the PU is available in the CR organize; the SU will promptly discharge the authorized bands as the PU has a selective benefit to utilize them (Yau, Komisarczuk, & Teal, 2009).

CR networks can be classified as the infrastructure-based CR network and the CRAHNs (Akyildiz, Lee, & Chowdhury, 2009). Since CRAHNs has no framework, a CR user can speak with other CR users through impromptu association on both authorized and unlicensed spectrum bands. Security and secrecy are the real necessities in any cognitive radio correspondence. Secrecy limit of the Multiple-Input Single-Output (MISO) cognitive radio channels was examined in (Pei, Liang, Zhang, Teh, & Li, 2010) where two numerical methodologies were proposed to determine the optimal transmit covariance matrix. The primary approach exchanged the original quasi-convex problem into a single convex semi-definite program while the second one exchanged the first semi-curved problem into a grouping of enhancement problems which demonstrates that, beamforming is the optimal strategy for the protected MISO cognitive radio channel. The secrecy limit of a cognitive radio system with numerous primary users, secondary users and eavesdroppers were considered in (Shu, Yang, Qian, & Hu, 2011) based on the stochastic geometry conveyances. The Poisson process was computed for both the secondary users and the eavesdroppers and it was shown, how the stochastic obstructions generated from secondary users can impact the secrecy limit of the primary users. The secrecy rate of a relay channel comprises of a source, a destination, and an eavesdropper was examined in (Dong, Han, Petropulu, & Poor, 2010) with Cooperative Jamming (CJ) and it was demonstrated that CJ plan can essentially enhance the secrecy rate of wireless channels. The CJ was contemplated in (Zheng, Choo, & Wong, 2011) to build the physical layer security of fading channels by means of distributed relays and it was demonstrated that the optimal CJ solution can be obtained by a combination of convex optimization and one-dimensional search. This approach could be utilized for improving the SMOR model; however, while adapting for CRAHN the secrecy rate of the secondary users is affected by the interferences from the primary users.

Lin, & Chen, (2014) have been developed SMOR model as an efficient opportunistic routing model but has many limitations which are highlighted in (Abdullah, & Kumar, 2015). We have developed improved routing models based on SMOR namely, modified SMOR (M-SMOR) model (Abdullah, & Kumar, 2017a), Sparsity-based distributed spectrum map SMOR, Optimization based SMOR (OCS-M-SMOR) (Abdullah, & Kumar, 2018a), and vertex search based energy efficient SMOR (VS-M-SMOR) model (Abdullah, & Kumar, 2018b). Additionally, Hybrid Artificial Bee Colony based SMOR (Abdullah, & Kumar, 2016) and Hybrid Bat based SMOR (Abdullah, & Kumar, 2017b) have also been developed. However, considering the security, there has not a wide gap in these methods that needs further enhancements. In order to improve security in communication without any interference as said above, this chapter modifies SMOR model using SCJ based relay selection and Blowfish encryption algorithm to develop

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/selective-cooperative-jamming-based-relay-selection-and-blowfish-encryption-for-enhancing-channel-and-data-security-in-crahn-routing/214808

Related Content

Vehicle Location and Navigation Systems
Ben-Jye Chang (2010). *Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications (pp. 119-130).*
www.irma-international.org/chapter/vehicle-location-navigation-systems/39523

Hadoop-Based Distributed K-Shell Decomposition for Social Networks
Katerina Pechlivanidou, Dimitrios Katsarosand Leandros Tassiulas (2018). *Graph Theoretic Approaches for Analyzing Large-Scale Social Networks (pp. 125-145).*
www.irma-international.org/chapter/hadoop-based-distributed-k-shell-decomposition-for-social-networks/186305

SEF4CPSIoT Software Engineering Framework for Cyber-Physical and IoT Systems
Muthu Ramachandran (2021). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-24).*
www.irma-international.org/article/sef4cpsiot-software-engineering-framework-for-cyber-physical-and-iot-systems/267220

Hyper Connectivity as a Tool for the Development of the Majority
Danilo Piaggesi (2021). *International Journal of Hyperconnectivity and the Internet of Things (pp. 63-77).*
www.irma-international.org/article/hyper-connectivity-as-a-tool-for-the-development-of-the-majority/267223

Social Cybersecurity and Human Behavior
S. Raschid Mullerand Darrell Norman Burrell (2022). *International Journal of Hyperconnectivity and the Internet of Things (pp. 1-13).*
www.irma-international.org/article/social-cybersecurity-and-human-behavior/305228