International Journal of Wireless Networks and Broadband Technologies
Volume 6 • Issue 2 • July-December 2017

Detection of PUE Attack in CRN with Reduced Error in Location Estimation Using Novel Bat Algorithm

Aasia Rehman, Kashmir University, Srinagar, India
Deo Prakash, Shri Mata Vaishno Devi University, Katra, India

ABSTRACT

Cognitive Radio Network Technology makes the efficient utilization of scarce spectrum resources by allowing the unlicensed users to opportunistically use the licensed spectrum. Cognitive Radio Network due to its flexible and open nature is vulnerable to a number of security attacks. This paper is mainly concerned with one of the physical layer attack called Primary User Emulation Attack and its detection. This paper solves the problem of PUE attack by localization technique based on TDOA measurements with reduced error in location estimation using a Novel Bat Algorithm (NBA). A number of cooperative secondary users are used for detecting the PUEA by comparing its estimated position with the known position of incumbent. The main goal of NBA is to minimize two fitness functions namely non-linear least square and the maximum likelihood in order to optimize the estimation error. After evaluation, simulation results clearly demonstrates that NBA results in reduced estimation error as compared to Taylor Series Estimation and Particle Swarm Optimization.

KEYWORDS

Cognitive Radio, Cognitive Radio Networks, Maximum Likelihood, Non-Linear Least Square, Novel Bat Algorithm, Primary User Emulation Attack, Taylor Series Estimation, Time Difference of Arrival

1. INTRODUCTION

Today the need for more spectrum bands is increasing rapidly as more wireless applications are being developed. Studies about spectrum have concluded that the licensed spectrum band is most of the time underutilized (Yuan et al., 2012) because of the classical allocation strategies used for spectrum which allocates a large portion of spectrum to licensed devices and at the same time not allowing the unlicensed devices to use the spectrum even though the licensed devices are not fully exploiting the licensed spectrum. Cognitive Radio Technology is an emerging technology that mitigates the issue of spectrum scarcity by allowing the unlicensed devices to exist side by side along with licensed devices. In this new technology the cognitive radio, i.e. unlicensed users opportunistically exploit the white spaces in the licensed spectrum band for communication purposes as long as they do not cause any interference to licensed user i.e. incumbent users, thus ensures the efficient utilization of spectrum. However, if any incumbent activity appears in the channel in which the secondary users are currently operating, they must perform spectrum handoff i.e. move to another vacant band. On the other hand, if other CR user is also transmitting in the same band then self-coexistence techniques are required for sharing the band. Cognitive Radio differs from the traditional radio in the sense that it has the ability of sensing the radio environment and then changes its operating parameters according

DOI: 10.4018/IJWNBT.2017070101

to the sensed data from the environment. Cognitive Radio Networks are sensitive to various attacks at different layers of OSI model (El-Hajj et al., 2011) as shown in Table 1:

This paper discusses the Primary User Emulation Attack which is a physical layer attack. Primary User Emulation attack was initially made known by (Chen & Park, 2006, pp. 110–119), in which the malicious node either repeats or imitates the features of incumbent signals e.g. type of modulation, transmission power and sends the signal to the network in order to refrain the secondary users from taking advantage of vacant channels. Current spectrum sensing techniques like matched filter and cyclo-stationary feature detection are not capable of identifying primary user emulation attack as the malicious node can send the signals with similar cyclic prefix and characteristics of primary signal. Hence effective methods need to be introduced to distinguish among the genuine primary signals and the false ones. Detection methods for PUE attack have been introduced mainly for standard IEEE 802.22 wireless regional area networks (WRAN) which may have two types of incumbents as: TV transmitters and wireless microphones.

Here we first apply a cooperative mechanism to detect the primary user emulation attacker in IEEE 802.22 CR networks. Each and every secondary user first performs spectrum sensing and transmits the sensing results to the base station, which implements a cross correlation technique to obtain TDOA measures. These TDOA values are utilized to obtain the position of the source of the transmitted signal which can either be a genuine incumbent i.e. TV tower or a primary user emulation attacker. Then an optimization algorithm known as Novel Bat Algorithm (NBA) is used in order to enhance the accuracy of the location estimation and also to decrease the time to locate the attacker with reduced number of secondary users required to reveal the PUE attacker, by minimizing the Non-linear least square cost function and maximum likelihood cost function.

2. PRIMARY USER EMULATION ATTACK IN COGNITIVE RADIO NETWORKS

PUE attack is defined as where the attacker changes its frequency of transmission to follow the signal characteristics of the incumbent and makes the secondary users believe that it is the legitimate primary user signal. As a result, secondary users perform spectrum handoff. PUE attack can adversely affect the spectrum sensing mechanism and also decreases the availability of channel to the secondary users extremely (Yu et al.). Figure 1 shows the scenario of primary user emulation attack Here we have two bands of spectrum Licensed band I and Licensed band II each having six channels $f_{1,}$ $f_{2,}$ $f_{3,}$ $f_{4,}$ $f_{5,}$ f_6 and $f_{7,}$ $f_{8,}$ $f_{9,}$ $f_{10,}$ $f_{11,}$ f_{12} respectively. First take an example in Licensed band I in which three channels namely f_1, f_3 and f_4 are used by primary system to send the signals to the primary receiver. The remaining f_2, f_5 and f_6 channels are free which are allowed to be used by the secondary users SU_1, SU_2 and SU_3 for communication. But if a PUE attack occurs e.g. EU_2 may disallow the secondary users from using the free channels by emulating the signal transmitted by the primary user in the channel f_2. As a result of PUE attack the secondary users are made to leave the corresponding channel. Now take the example in licensed band II in which the primary system uses the channels f_{11} and f_{12} and the channels f_9 and f_{10} are used by secondary users SU_4 and SU_5 respectively and the EU_3 and EU_4 attackers mimics the

Table 1. Various Layers and Corresponding Attacks on them

S.no.	Layers	Attacks
1.	Physical Layer	PrimaryUser Emulation, Objective Function Attack, Jamming
2.	Data Link Layer	spectrum sensing data falsification, control channel saturation DoS, selfish channel negotiation
3.	Network Layer	Sink hole attack, Sybil attack, Wormhole attack
4.	Transport Layer	Key Depletion Attack