Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 21 (2013) 430 – 435

Procedia Computer Science

2013 International Workshop on Communications and Sensor Networks (ComSense-2013)

Detecting Primary User Emulation Attacks in Cognitive Radio Networks via Physical Layer Network Coding

Xiongwei Xie[a], Weichao Wang[a]

[a]*Department of SIS*
UNC Charlotte
Charlotte, NC 28223
Email: xxie2@uncc.edu, weichaowang@uncc.edu

Abstract

Primary user emulation (PUE) attacks on cognitive radio networks pose a serious threat to the deployment of this technique. Previous approaches usually depend on individual or combined received signal strength (RSS) measurements to detect emulators. In this paper, we propose a new mechanism based on physical layer network coding to detect the emulators. When two signal sequences interfere at the receiver, the starting point of collision is determined by the distances among the receiver and the senders. Using the signal interference results at multiple receivers and the positions of reference senders, we can determine the position of the 'claimed' primary user. We can then compare this localization result with the known position of the primary user to detect the PUE attack. We design a PUE detection mechanism for wireless networks with trustworthy reference senders. We analyze the overhead of the proposed approach and study its detection accuracy through simulation.

Keywords: primary user emulation, physical layer network coding, cognitive radio networks

1. Introduction

The dynamic spectrum access technique allows wireless nodes to use spectrum sensing to identify the 'white spaces' in licensed spectrum. The cognitive radios will then opportunistically utilize these white spaces. To avoid any interference with the primary users, a secondary user must leave the occupied channels if it detects a primary user. Therefore, one of the major technical challenges in spectrum sensing is the problem of precisely identifying the signals of the real primary users. The malicious secondary users can mimic the spectral characteristics of primary users to gain priority access to the wireless channels, which is called "primary user emulation" (PUE) attacks.

Existing approaches to detecting the PUE attacks can be divided into two groups: communication oriented and localization oriented. In the first group, the secondary nodes use the spectrum sensing techniques to match the characteristics of the radio signals to those of the primary user. The detection mechanisms include filter and cyclostationary feature detection [1], spectrum decision and channel parameters [2], and shadow senders [3]. In the second group, the researchers use the received signals to estimate the position

doi:10.1016/j.procs.2013.09.057

of the sender. They have designed different methods to model the communication channels and improve the signal measurement accuracy [4]. Outliers in localization procedures are filtered out to improve the detection accuracy of PUE attacks [5].

In this paper, we propose a PUE attack detection mechanism based on the physical layer network coding (PNC) technique. PNC uses the additive nature of the electromagnetic waves to serve as the coding procedure. In our approach, we estimate the position of a wireless node by letting its radio signals interfere with a reference sender. These interfered sequences will be captured by multiple secondary users. Combining the starting points of signal interference results with their positions, the secondary users will determine a group of hyperbolas on which the wireless sender resides. Then they will compare the intersection point of these hyperbolas with the known position of the primary user to detect the PUE attack.

To turn the approach into a practical solution, research challenges from multiple aspects must be carefully addressed. From the network point of view, we need to verify the authenticity of the received signals and accurately locate the position of the sender. From the security point of view, we need to design mechanisms to identify the false claims of positions and signal interference results provided by malicious nodes.

Our investigation has the following contributions: (1) The research will demonstrate that in addition to improving the bandwidth usage efficiency in wireless networks, physical layer network coding can also be used to detect malicious attacks. (2) The proposed PUE attack detection mechanism does not require the deployment of any special hardware. The assumed trustworthy reference senders already exist in the IEEE standards such as 802.22 and 802.16h. (3) The overhead and detection accuracy of the approach are studied through both theoretical analysis and simulation.

The remainder of this paper is organized as follows. In Section 2, we introduce the basic idea of using PNC for localization. In Section 3, we present the details of the proposed approach. The overhead and detection accuracy of the approach are studied in Section 4. Finally, Section 5 concludes the paper.

2. Localization through Physical Layer Network Coding

2.1. System Assumptions

We assume that the primary user (e.g. a TV station) is located at a fixed position and both the secondary users and the attackers know its position. Since FCC requires all TV towers or radio stations to enforce strict physical security, we assume that the secondary users or the attackers cannot be physically close to the primary user. We assume that all secondary users are equipped with GPS and a secure, lightweight pseudo random bit generator (PRBG) [6]. The authenticity and integrity of the packets are protected by the Message Authentication Code (MAC). The details of packet authentication will be discussed in Section 3.

We assume that the attackers also have the GPS device and the PRBG. An attacker can mimic a primary user's radio signals. Multiple attackers can collaborate to conduct a PUE attack. However, the attackers do not have the computation power to compromise the encryption keys or reverse a secure hash function.

2.2. Use PNC to Achieve Localization

Figure 1 illustrates the basic idea of physical layer network coding. In the topology, A and C depend on B to forward the frames between them. In the PNC approach, A and C will send out their packets and B will receive the interference results of the two frames. It will rebroadcast the received signals to both A and C so that they can leverage their knowledge about $frame1$ and $frame2$ respectively to separate the signals and recover the data. Please note that the PNC based mechanism does not require the frames to reach the receiver simultaneously since it can accurately locate the starting point of signal collisions [7].

We can use PNC to calculate the position of a wireless node. We use d_{MN} to represent the distance between two nodes M and N. We use T to represent a specific moment and t to represent a time duration. If radio waves propagate at the speed s, the transmission delay between M and N will be $\frac{d_{MN}}{s}$. In our analysis, we measure the difference between the arriving time of two sequences based on the starting point of signal collisions. We can locate the symbol in the sequence from which the collision starts. Then we can translate this information into a time difference based on the frequency of the radio signals.