Journal of Network and Computer Applications 72 (2016) 140–149

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Supporting secure spectrum sensing data transmission against SSDH attack in cognitive radio ad hoc networks ☆

Jingyu Feng [a,b], Guangyue Lu [a,*], Honggang Wang [a], Xuanhong Wang [a]

[a] *Department of Communication Engineering, Xi'an University of Posts and Telecommunications, Xian 710121, China*
[b] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*

ARTICLE INFO

Article history:
Received 22 December 2015
Received in revised form
2 June 2016
Accepted 14 June 2016
Available online 18 June 2016

Keywords:
Cognitive radio
Ad hoc
Cooperative spectrum sensing
Hijack
Trust

ABSTRACT

Cognitive radio ad hoc networks are commonly perceived as ideal ad hoc environments where cognitive radio technology enables secondary users (SUs) to utilize scarce spectrum resources in a dynamic manner. Cooperative spectrum sensing (CSS) is the key function of cognitive radio technology to identify the available spectrum. However, the nature of aggregating data makes CSS offer opportunities for malicious SUs. Recently, a lot of efforts have been paid to combating spectrum sensing data falsification (SSDF) threat, but little attention to the multi-hop architecture of cognitive radio ad hoc networks. In this paper, we report the discovery of a novel attack called spectrum sensing data hijack (SSDH), in which attackers disguise as routers to hijack and tamper with spectrum sensing data during the transmission. Our simulations show that this new attack needs much less cost to manipulate CSS and has a much higher success rate compared with SSDF attack. We conduct an in-depth investigation on SSDH and propose a two-level defense scheme from the design ideas of IBC signature-verification and neighbor monitor. We also perform simulations to validate our approach. The results show that our defense scheme can significantly reduce the SSDH attack success ratio.

1. Introduction

With the rapid development of wireless communication and the huge demand of the capacity for wireless applications, the wireless frequency spectrum has become increasingly scarce. At the same time, a large portion of the assigned spectrum bands, such as in the 400–700 MHz range, that are used sporadically or under-utilized for transmission (Federal Communications Commission, 2002). To solve the contradiction between the spectrum scarcity and low spectrum utilization, cognitive radio has been considered as a useful technology. Currently, cognitive radio technology is introduced in ad hoc networks, and thus forming cognitive radio ad hoc networks (CRAHNs) which refer to the distributed networks where unlicensed user (or Secondary User-SU) can share the spectrum with licensed user (or Primary User-PU) if they do not cause any interference to PU (Le The Dung and Beongku, 2002). CRAHNs are gaining importance with the increasing number of potential applications, such as military battlefield communications, disaster relief, and autonomous vehicular communications (Akyildiz et al., 2009).

Cooperative spectrum sensing (CSS) is the key function of cognitive radio technology to enhance the detection performance by exploiting spatial diversity via the observations of spatially located SUs. In a CSS architecture, all the participating SUs forward their observations regarding the presence or absence of a PU to a fusion center (FC), which makes the final decision about whether the PU is transmitting or not. This nature of aggregating data makes CSS offer opportunities for malicious SUs to launch SSDF (Chen et al., 2008) attack by sending false spectrum sensing data. For convenience, spectrum sensing data are abbreviated as sensing data in the rest of this paper.

Fortunately, SSDF attack can be suppressed by trust mechanism and many efforts have been made to study various trust mechanisms (Qin et al., 2009; Zeng et al., 2014; Feng et al., 2015; Pei et al., 2013). They estimate whether an SU is trustworthy or not by its past behaviors and give low weights to the sensing data from less trustworthy SUs when generating a final decision. In addition, it may be a huge task for malicious SUs to launch SSDF attack since a malicious SU can only fake one sensing datum at each CSS action. That is, to change the final decision from CSS, a sufficient number of malicious SUs are necessary.

☆This research was supported in part by the National Science Foundation of China (61301091, (61271276), the Open Foundation of State Key Laboratory of Information Security (2015-MS-14), the Industrial Science and Technology project of Shaanxi Province (2014K05-09, 2015GY013), the Natural Science Foundation of Education Department of Shaanxi Province (14JK1660), the China Postdoctoral Science Foundation(2015M582622), the New Star Team of Xian University of Posts & Telecommunications.

* Corresponding author.
E-mail address: tonylugy@163.com (G. Lu).

http://dx.doi.org/10.1016/j.jnca.2016.06.007
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

Note that CRAHN protocols follow message forwarding mechanisms in CSS, where the SUs with strong report channel can serve as relays to assist in forwarding sensing data from the SUs with weak report channel (Akyildiz et al., 2011). In this paper, we discover a novel attack along this line, named as spectrum sensing data hijack (SSDH), against CSS in CRAHNs, and propose a two-level defense scheme called GSSD from the perspective of guarding spectrum sensing data during the transmission to defend against this attack. The main contributions of this paper are as following:

- Conduct an in-depth investigation on SSDH attack, including four types of threats, attack strategy and attack power. Compared with SSDF attack, SSDH needs less cost to achieve the similar goals. The basic idea of SSDH is as follows. SSDH attackers disguise as routers to hijack and tamper with sensing data from the SUs who can sense PU signal. As a result, the SUs who require sensing data will make a wrong final decision, but the SUs who sensed PU signal may be considered as dishonest and their trustworthiness will be reduced since their sensing data disagree with PUs actual status. Nevertheless, SSDH attackers get away with punishment.
- Use IBC signature-verification as the first level defense scheme. It is difficult to adopt the public key cryptography (PKC) to encrypt or sign sensing data since no a central authority can be employed to manage key exchange. We design the first level defense scheme based on the identity-based cryptography (IBC) (Shamir). This scheme asks the SUs who can sense PU signal to sign sensing data with their private keys and produce a digital signature. This signature confirms the authenticity and integrity of sensing data, and thus increasing the difficulty of launching SSDH attack.
- Introduce the design idea of neighbor monitor as the second level defense scheme. Three advantages can be found in the second level defense scheme: identifying tampered sensing data, correcting sensing data and isolating SSDH attackers. To identify tampered sensing data, the first level defense scheme is performed by each router (such as SU_i) to monitor his previous router (such as SU_p). If tampered, the neighbor tie value nt_{ip} generated from SU_i to SU_p will be reduced. Considering that one sensing datum is a binary variable {0, 1}, we ask that the behavior of forwarding tampered sensing data will also cause the decrease of nt_{ip} for SU_p. This stimulates SU_p corrects sensing data when finding his neighbors who tampered with these data. By neighbor monitor, SSDH attackers will get bad neighbor tie value from his neighbors who have the right to refuse to forward SSDH attackers' CSS help query. In this case, SSDH attackers can be isolated from CSS.

2. Preliminaries

2.1. Cooperative spectrum sensing

In the CRAHNs, SUs cooperate with each other to achieve a CSS exchange in the self-organizing manner due to the lack of centralized control. As shown in Fig. 1, when an initiator SU (such as SU_0) wants to know the spectrum status of the target PU in a CRAHN, a CSS exchange will be trigged: individual sensing, data reporting and data fusion.

- *Individual sensing*: Each SU senses the vacant spectrum of the PU via the sensing channel individually. The sensing channel is the selected licensed frequency band where a physical point-to-point link between the PU transmitter and each cooperating SU is employed to observe the primary spectrum (Akyildiz et al., 2011).

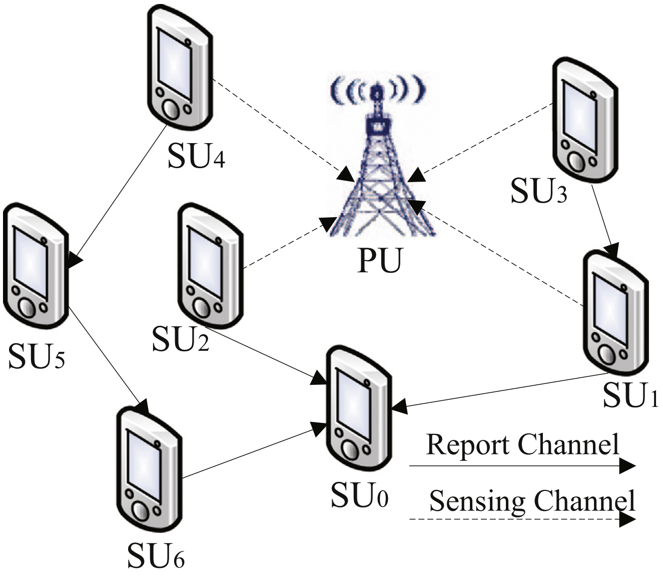

Fig. 1. The CSS exchange launched by SU0 in a CRAHN.

- *Data reporting*: All SUs send their sensing data to SU_0 via the report channel. The reporting channel is a control channel where a physical point-to-point link between each cooperating SU and the initiator SU is employed to send individual sensing information (Akyildiz et al., 2011). If both sensing channel and reporting channel are not perfect, an SU observing a weak sensing channel and a strong report channel and another SU with a strong sensing channel and a weak reporting channel, for example, can complement and cooperate with each other to improve the performance of CSS. In Fig. 1, SU_3 and SU_4, who observe strong PU signals, may suffer from a weak reporting channel. SU_1, SU_5 and SU_6, who have a strong reporting channel, can serve as relays to assist in forwarding the sensing data from SU_3 and SU_4 to SU_0.
- *Data fusion*: Without a central authority, SU_0 combines the received sensing data and to determine the final decision of PU spectrum. The final decision are usually made according to three typical CSS fusion rules, such as the "AND", "OR" and "Majority" rule (Peh et al., 2009).

Typically, individual sensing for primary signal energy detection can be formulated as a binary hypothesis problem as follows (Akyildiz et al., 2009):

$$y(t) = \begin{cases} n(t), & H_0 \\ h(t)\cdot s(t) + n(t), & H_1 \end{cases} \tag{1}$$

where $y(t)$ represents the detected signal at each SU, $s(t)$ is the transmitted PU signal, $h(t)$ is the channel gain of the sensing channel, $n(t)$ is the zero-mean additive white Gaussian noise (AWGN), H_0 and H_1 denote the hypothesis of the absence and the presence of the PU signal, respectively. If the estimated energy of the received signal is larger than the decision threshold, the existence of PU would be declared. Otherwise, if the energy of the received signal is smaller than the threshold, there is no PU signal.

After the individual sensing, the individual sensing data of each SU is determined. d_i indicates the individual sensing data of SU_i, which is usually expressed as a binary variable:

$$d_i = \begin{cases} 0, & H_0 \\ 1, & H_1 \end{cases}$$

where "0" and "1" denote the hypothesis of the absence and the presence of the PU signal, respectively. The spectrum sensing