Signal Processing 137 (2017) 1–9

Contents lists available at ScienceDirect

Signal Processing

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

Probabilistic spectrum sensing data falsification attack in cognitive radio networks

Arash Ahmadfard, Ali Jamshidi*, Alireza Keshavarz-Haddad

School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran

ARTICLE INFO

Article history:
Received 26 October 2016
Revised 4 January 2017
Accepted 27 January 2017
Available online 29 January 2017

Keywords:
Cognitive radio networks
Cooperative spectrum sensing
Malicious sensors
Data falsification
Probabilistic attack

ABSTRACT

Cognitive radio has emerged as a solution to the problem of spectrum scarcity in recent years. Spectrum sensing is a key task in cognitive radio systems that can be performed collaboratively. Although collaboration enhances the performance of spectrum sensing, it can put the cognitive network in a vulnerable position. The cognitive users may send falsified reports, hence degrade the performance of spectrum sensing. In this paper, we propose a flexible structure which enables the attacker to reconfigure the attack parameters based on the defense strategy employed at the fusion center (FC) adaptively. In particular, we consider a cognitive network in which the cognitive users send their observations in a quantized format. It is assumed that a soft-decision-based defense strategy is employed at FC to detect the attackers. The attacker maps its quantized observations onto the other quantization levels probabilistically and reports them to FC. The attacker's objective is to perform probabilistic mapping such that the performance of FC degrades as much as possible. At the same time, the attacker considers the attack costs. We demonstrate that the proposed attack method leads to a convex linear programming problem. A low complexity algorithm is proposed to solve the problem. Simulation results are presented to show the effectiveness of the proposed scheme.

1. Introduction

Due to capability of improving spectrum utilization, cognitive radio has attracted intensive attention in recent years [1,2]. In cognitive radio networks, cognitive users (also known as secondary users) access the spectrum opportunistically whenever the licensed users (also known as primary users) are not present. The cognitive users change the channel being used whenever the primary users come back. The key task in cognitive radio systems is spectrum sensing in which the spectrum opportunities are obtained and the presence of primary users is detected.

Phenomena like channel fading can degrade the accuracy of spectrum sensing. Collaborative spectrum sensing is proposed in the literature to enhance the performance of spectrum sensing [3–5]. According to collaborative spectrum sensing, a fusion center (FC) collects the reports of cognitive users to make the final decision. Decision making can be either hard or soft. In the hard scenario, each cognitive user sends its local binary decision about the existence of the primary user, while in the soft scenario, it sends the value of the energy received from the primary user to FC.

Although collaboration enhances the accuracy of spectrum sensing procedure, it may put the cognitive networks in a vulnerable position. The cognitive users may send falsified reports to the FC, hence degrade the performance of spectrum sensing. The incentive for such behaviors is twofold: (i) The attacker is greedy. In this case, the attacker sends reports indicating the primary users are present while they are not. This misbehavior causes cognitive network to stop using the channel and the attacker utilizes the channel itself. This action leads to increase in false alarm probability of FC. (ii) The attacker is malicious. In this case, the attacker declares that the channels are idle while they are busy to make the cognitive users access the channels and cause interference to the primary users. This action leads to increase in the misdetection probability of the FC.

Three soft spectrum sensing data falsification (SSDF) attack models have been widely used to test various defense algorithms [6]: *Always-Yes* [7–11], *Always-No* [7,9], and *Always-Adverse* [7,11–14]. In Always-Yes attack model, the attacker reports a high value in every time-slot to increase the false alarm probability of FC. In Always-No attack model, the attacker always reports a low value to the FC to increase the misdetection probability of FC. In Always-Adverse case, the attacker makes decision about the existence of the primary user locally; if the primary user is detected to be present, the attacker reports a low value, else it reports a high

* Corresponding author.
E-mail addresses: ahmadfard@shirazu.ac.ir (A. Ahmadfard), jamshidi@shirazu.ac.ir (A. Jamshidi), keshavarz@shirazu.ac.ir (A. Keshavarz-Haddad).

http://dx.doi.org/10.1016/j.sigpro.2017.01.033
0165-1684/

value. The main limitation of these three attack models is that they are oversimplified. To overcome this problem, intelligent attacks are proposed in the literature for both hard and soft scenarios.

In [15], a hard SSDF attack model is considered. The paper assumes that FC can measure the trustworthiness of each cognitive user. The trustworthiness of a cognitive user is decreased once its behavior is detected to be abnormal. In addition, if this parameter decreases below a predefined threshold for a cognitive user, that user is excluded by FC from the final decision making process. In that work, an intelligent attack is addressed in which the attacker can predict its suspicious level computed by the FC. Once the suspicious level is close to a threshold, the attacker stops attacking and sends honest reports such that its suspicious level keeps falling. When the attacker feels safe, it launches attack again. With this strategy, the stealthiness of attacker is guaranteed.

In [16], an attack on the hard decision based spectrum sensing model is considered. The decision of each cognitive user has a binary value. The attacker maps zero to one or one to zero probabilistically such that the probability mass function (PMF) of the reports of the cognitive users at FC be the same for both cases where the primary user is absent and present, i.e., FC goes blind. To achieve this objective, the attacker tries to minimize Kullback Leibler divergence (KLD) between the two PMFs by a probabilistic mapping. KLD metric is used to quantify similarity between two PMFs and it is zero when the PMFs are identical [17].

In [6] and [18], an attack on the soft decision spectrum sensing model is considered in which the attacker makes decision about the presence of the primary user locally. Then, it falsifies the observation with probability p or reports the truth with probability $1-p$. When the attacker decides to attack, it takes action based on its local detector. If the observation is less than the threshold, a Gaussian random variable with mean value greater than the threshold is reported to FC. This action increases the false alarm probability of FC. In addition, when the observation is greater than the threshold, a Gaussian random variable with mean value less than the threshold is reported. This action leads to increase in the misdetection probability of the FC. In accordance with [6], the attacker must attack as aggressively as possible to cause the poorest performance of FC (Theorems 1, 2 and 3 in [6]). For instance, the attack probability p must be set as high as possible, i.e. $p=1$. Note that attacking aggressively increases the risk of being detected by FC. Apart from this, it is assumed that the number of attackers, the strategy of each of them, and the instantaneous weight allocated to each cognitive user for combining the reports at FC is available to a typical attacker which may not be true in general. Moreover, although the attack strategy in [18] is flexible, no algorithm is explained to set the attack parameters. In that work, it is not clear how to adjust the attack parameters such that the attack is effective, and at the same time, the risk of being detected by FC is acceptable.

In this paper, a novel attack on the soft decision spectrum sensing model is studied that is called *Probabilistic SSDF attack*. In this attack, the attacker is enabled to reconfigure its parameters adaptively. We assume that the cognitive users send their observations in a quantized format. For an honest user, the quantized level corresponding to its observation is reported to FC. However, an attacker may falsify its observations and map them onto other quantization levels probabilistically. The attacker's objective is to perform probabilistic mapping such that the performance of FC degrades as much as possible. At the same time, the attacker considers the attack costs. Based on our formulations, the attacker needs to solve a convex linear programming problem for choosing the attack parameters optimally. We prove that this optimization problem can be decomposed into a number of simple maximization problems. In addition, it is not necessary to solve all these maximization problems at a time in order to launch an effective attack. Finally, simulation results are presented to show the effectiveness of the proposed scheme.

Note that in contrast to the Always-Yes, Always-No, Always-Adverse and the attack strategies in [6] and [18], in this work, the PMF of the reports of the attackers is not restricted to have a specific form. Hence, these attack strategies are a special case of the proposed attack strategy. Moreover, in contrast to the existing works, we take the cost for falsification of the observations into account to control the aggressiveness of the attacker arbitrarily.

The rest of this paper is organized as follows: The system model is presented in Section 2. In Section 3, we describe the probabilistic SSDF attack model. Performance evaluation of the proposed attack model is studied in Section 4. Finally, we conclude the paper in Section 5.

2. System model and notations

We assume a primary network in which the users access the channels in a time-slotted fashion and a cognitive network with M users. The cognitive users opportunistically utilize the channels whenever they are idle. The cognitive users perform collaborative spectrum sensing to figure out presence or absence of primary users over different time-slots. A fusion center gathers sensing information by the cognitive nodes to make the final decision on spectrum sensing results (as depicted in Fig. 1).

Each cognitive user samples the received signal. When the primary user is inactive, the energy measured at the kth time-slot by the mth cognitive user is given by:

$$u_m(k)=\frac{1}{N}\sum_{i=1}^{N}|\nu_m(k,i)|^2, \tag{1}$$

where $\nu_m(k,i)$ is the received noise by the mth cognitive user in the ith sample of the kth time-slot and N is the number of samples taken by the cognitive user. When the primary user is active, $u_m(k)$ will be:

$$u_m(k)=\frac{1}{N}\sum_{i=1}^{N}|h_m(k,i)s(k,i)+\nu_m(k,i)|^2, \tag{2}$$

where $h_m(k,i)$ is the channel gain between the primary and the mth cognitive user and $s(k,i)$ is the signal of the primary user at the ith sample of the kth time-slot. Let $h_m(k,i)$ be constant over time, i.e. $h_m(k)=h_m(k,i)$.

We assume the noise samples $\nu_m(k,i)$ are independent identical distributed with complex Gaussian distribution, i.e. $\nu_m(k,i)\sim\mathcal{CN}(0,\sigma^2)$. In accordance with the central limit theorem, $u_m(k)$ asymptotically follows Gaussian distribution if N is large, say $N\geq 10$. Depending on the presence or absence of the primary user, the pdf of $u_m(k)$ is different. Consequently,

$$u_m(k)\sim\begin{cases}\mathcal{N}(\mu_0,\sigma_0^2), & H_0 \quad (3a)\\ \mathcal{N}(\mu_1,\sigma_1^2), & H_1 \quad (3b)\end{cases}$$

where $\mu_0=\sigma^2$, $\sigma_0^2=\frac{\sigma^4}{t}$, $\mu_1=(\gamma_m(k)+1)(t)$, $\sigma_1^2=\frac{(2\gamma_m(k)+1)\sigma^4}{t}$, and $\gamma_m(k)=\frac{|h_m(k)|^2}{\sigma^2}$ (for more details see [19,20]). In the above formula, H_0 and H_1 denote the case that the primary user is inactive and active, respectively.

The cognitive users quantize their observations $u_m(k)$ before reporting them to FC due to bandwidth limitations of the communication channel. Let $\hat{u}_m(k)$ and $r_m(k)$ denote the quantized value and the value of sent report corresponding to $u_m(k)$. Moreover, let $E_1<E_2<\cdots<E_L$ be the L quantization levels. From FC's point of view, any cognitive user is a potential attacker. Clearly, a cognitive user is honest if $r_m(k)=\hat{u}_m(k)$ and it is attacker if $r_m(k)=\hat{u}_m(k)$.

Let α_i be the probability that the cognitive user's quantized observation is E_i when the primary user is absent. Similarly, β_i