Ad Hoc Networks 11 (2013) 2367–2380

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

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

Detection of malicious users in cognitive radio ad hoc networks: A non-parametric statistical approach

Ferran Adelantado [a,*], Christos Verikoukis [b]

[a] IT, Multimedia and Telecom Department, Open University of Catalonia, Rambla Poblenou, 156, Office 205, 08018 Barcelona, Spain
[b] Telecommunications Technological Centre of Catalonia, Av. Carl Friedrich Gauss 7, 08860 Castelldefels, Spain

ARTICLE INFO

Article history:
Received 22 January 2013
Received in revised form 25 May 2013
Accepted 17 June 2013
Available online 27 June 2013

Keywords:
Cognitive radio ad hoc network
MAC layer security
Malicious user detection
Kruskal–Wallis test

ABSTRACT

Cognitive radio ad hoc networks (CRAHN) operation is based on the reliability of the spectrum sensing. It has been proved that cooperation between secondary users improves the accuracy of the sensing information gathered by the users. However, such cooperation also increases the vulnerability of the network and its exposure to attacks. The paper presents a novel algorithm based on the non-parametric Kruskal–Wallis and Conover–Inman tests to detect and identify the attack of malicious users at the MAC layer. The algorithm, denoted by KWD, does not assume a priori knowledge neither of the activity of the primary channel nor of the existence and the behavior of malicious users.

1. Introduction

The wireless spectrum allocation and usage has been long characterized by static policies [1]. The availability of spectrum resources, as well as the difficulties in the generalization of a new spectrum allocation paradigm, deterred the involved agents (e.g. network operators, manufacturers, license holders or regulators) from facing spectrum allocation policies based on dynamic assignment [2].

The proliferation of wireless communication systems and the increase in the demand of wide band wireless services, together with the wireless resource scarcity, has shifted the focus onto the inefficiency of the traditional static spectrum allocation policy. In this context, the emergence of the Cognitive Radio (CR) concept [3], and particularly the Opportunistic Spectrum Sharing (OSS) concept [4], has set up the basis of a new spectrum usage paradigm.

OSS is based on two main premises: the maximization of the spectrum usage and the protection of the incumbent primary systems. Both premises are highly coupled and depend on the accurate knowledge of the nearby wireless environment, i.e. the detection of primary users (PU) transmitting/receiving in the vicinity of the secondary users (SU).

In cognitive radio ad hoc networks (CRAHN), the SUs are assumed to be able to detect and identify the energy transmitted by the PUs, process the information and proceed accordingly [4]. However, such capabilities are limited in nature and the SUs present non-null false alarm and missed detection probabilities [5]. Both inadequacies, i.e. false alarm and missed detection, affect the two premises on which OSS is based. Whereas false alarm diminishes the spectrum usage efficiency, missed detection endangers the protection of the incumbent PUs. In the aforementioned context, the cooperation among SUs comes up as a proper manner to improve the environment knowledge obtained during the sensing process [6]. However, although cooperation is effective to smooth the effect of sensing errors, it turns out to be inefficient to cope with the attacks of malicious SUs [7]8. Thus, cooperation poses new vulnerabilities, since false information might be easily propagated across the secondary network. In order to limit the impact of inaccurate/false sensing information, malicious SUs detection mechanisms are required.

* Corresponding author. Tel.: +34 933 263 539; fax; +34 933 568 822.
E-mail address: ferranadelantado@uoc.edu (F. Adelantado).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.06.002

2. Previous work and motivation

The existence of malicious SUs that provide false sensing information may degrade the performance of the cognitive wireless network. It is necessary, then, to develop mechanisms to detect and discard the sensing information provided by the malicious SUs, thereby preventing the network from such attacks.

The importance of the reliability of the SUs at the MAC layer level has attracted the interest of the research community. In particular, [7,8] are outstanding works where most of the main OSS security threats, at all layers, are analyzed and referenced. Focusing on the malicious users' MAC layer attacks, there are two main different strategies to cope with the problem. On the one hand, the processing of the cooperative information in order to mitigate its influence on the final spectrum occupancy decision, e.g. [9]. On the other hand, the detection and discarding of malicious users [10–15]. This paper is a contribution to the latter.

In the literature some proposals to detect malicious secondary users performing the so-called Bizantine attack have been presented, but they were restricted to scenarios where users had non-complex behavior patterns, such as always yes/no strategies [10] or an always false information strategy [11]. Additionally, the detection was limited to attacks performed by a single SU or few SUs [12]. Also more complex malicious behavior patterns have been studied, but restrictive assumptions were imposed. In [13] the whole study was based on the assumption that the fusion center was aware of the existence of an attack, and in [14] Wang et al. presented an approach to assign a trust value to each SU. However, missed detection and false alarm probabilities were supposed to be known a priori. Similarly, Chen et al. proposed in [15] a centralized algorithm (SCSS), based on the Weighted Sequential Probability Ratio Test (WSPRT), to address the same problem. In this case, the algorithm required accurate information on the location of the nodes.

Some works have also addressed the combination of sensing information [16–19] or the selection of the best SU's performance [20], although in all of them assumptions were too restrictive (assumptions on location or on the normality of the data distribution).

In this paper, a new algorithm based on statistical nonparametric methods is proposed to detect the malicious SUs. In the context of cognitive wireless ad hoc networks, the assumptions regarding the knowledge of the primary channel activity have a huge impact on the feasibility of the proposals. Hence, there are two hypothesis that limit the real application of the detection mechanisms: the knowledge on the existence of malicious SUs (and the characteristics of such attack) and the knowledge of the primary channel activity. This work analyzes the impact of malicious SUs and proposes a technique to identify what users are more reliable and what other users are less reliable, i.e. malicious users. The key point of the proposal is that no a priori knowledge is assumed. One of the most aligned works in the literature is [21], subsequently improved in [22], where assumptions on a priori knowledge are not imposed. There were, however, explicit and implicit limitations, since the design was based on the assumption of a reduced number of attackers. Similarly, a statistical algorithm called Conditional Frequency Check (CFC) is proposed in [23], also with a priori knowledge restrictions for an optimal performance. Some of these proposals are compared in the Numerical results section.

This paper is an extension of a preliminary work [24], in which the basic idea was stated. Additionally, formal proofs are derived in order to establish the correctness of the assumptions and the limits of the proposal, as well as to address the complex scenarios case. The main contributions of this work can be summarized as follows: (i) A new algorithm for malicious and misbehaving users' detection is proposed; (ii) No assumptions on the existence of malicious users' attacks are done; (iii) The algorithm is not restricted to a maximum number of malicious users; (iv) No a priori information on the characteristics of the users is required, neither from the malicious users nor from the honest users; and (v) The algorithm need not know the PUs activity pattern.

The paper is organized as follows: First the problem is modeled and the operation of all the involved agents is described in Section 3. In Section 4 the impact of the malicious users on the decision of the cognitive network is analyzed and in Section 5 the theoretical basis of the detection algorithm and the practical implementation of the algorithm itself are described. Simulation results are exposed in Section 6 and finally, in Section 7, the conclusions are presented.

3. System model

In the CRAHN under study, a cluster is defined as a set of $K+1$ secondary users, $U = \{u_k : 0 \leqslant k \leqslant K\}$, that sense the spectrum cooperatively. One of the SUs undertakes the role of the cluster head, while the rest of the SUs are referred to as sensors. For the sake of simplicity, and without loss of generality, u_0 is assumed to be the cluster head hereinafter.

The cooperative sensing procedure operates as follows. Every time a cooperative sensing process is triggered, the K sensors sense a set of primary channels, denoted by $F = \{f_m : 1 \leqslant m \leqslant M\}$. Then, the sensing information collected by the sensors is shared with the cluster head over the CCC (Common Control Channel), namely f_0. Upon the reception of the sensors' information, the cluster head combines the received information and broadcasts the result to the rest of the SUs within the cluster, also over the CCC. The CCC is generally an out-of-band secondary channel used for signaling and cooperation purposes, e.g. [25]. The design of the CCC is a challenging research topic itself, and in [26] some interesting solutions are presented. The exchange of sensing reports, from the sensors to the cluster head, can be subject to reception errors caused by fading. However, some of the proposals mentioned in [26] allow retransmission mechanisms. Accordingly, our proposal algorithm is designed on the basis of a reliable CCC existence.

3.1. Primary channel model

A primary channel may be modeled by its activity. The activity of a channel is defined by the random process $\{A(t); t \in \mathbb{R}_+\}$, where $A(t) \in \{0,1\}$. If the channel is *idle* at