Resilient and Multi-dimensional Cooperative Spectrum Sensing on Cognitive Radio Networks

Julio Soto and **Michele Nogueira**
Department of Informatics
Federal University of Paraná, Brazil
Emails: {soto,michele}@inf.ufpr.br

Kaushik Roy Chowdhury
Electrical and Computer Eng. Department
Northeastern University
Email: krc@ece.neu.edu

***Abstract*—While great strides have been made in spectrum sensing techniques in cognitive radio networks, these approaches are susceptible to unconventional attacks that may result in catastrophic performance degradation of the spectrum usage efficiency. For example, primary user emulation, intelligent jamming and denial of service for spectrum usage may impact the performance of classical spectrum sensing approaches. To address these challenges, this paper proposes a multi-dimensional cooperative sensing framework that can flexibly incorporate a variety of physical layer features to identify cases related to malicious behavior and genuine node failures. Though our approach is distributed, it is resilient in the sense that it does not simply rely on majority voting by a collection of nearby nodes. The key contributions of this paper are as follows: (i) A multiple criteria analysis technique and a non-parametric Bayesian inference method are formulated for identifying the spectrum holes that are least susceptible to malicious activity and failures, and (ii) Using real traces from the CRAWDAD data repository, we test our framework in a variety of practical settings, to prove the performance benefit of our approach.**

I. Introduction

Cognitive radio (CR) is the enabling technology that allows unlicensed secondary users (SUs) to exploit idle licensed frequency bands, forming thus a cognitive radio network (CRN). CRs can autonomously adjust their transmission parameters and modify their behavior based on the electromagnetic environment conditions. Spectrum sensing is a key phase in the operation cycle of a CR [1], leverating the radio's ability to measure, sense and be aware of the channel characteristics. It can be performed either individually or cooperatively in order to detect idle frequencies, referred to as *spectrum holes*, and minimize interference to the licensed or primary user (PU) activities [2]. The accuracy on detecting spectrum holes determines the efficiency of exploiting the spectrum. Thus, either sensing errors related to hardware outages [3], [4] or susceptibility to specialized attacks on the sensing functionality can result in significant performance degradation.

Existing works on security in CR mainly address concerns of designs for cryptography, intrusion detection system and authentication. However, these security measures are not sufficient to preserve the correctness of spectrum sensing results against attacks and intrusions [4]. Preventive security mechanisms, as cryptography, provide confidentiality, integrity and authentication, but they are inefficient against data injection overload, interception, manipulation or impersonation attacks, such as Denial of Services (DoS), PU emulation (PUE) attacks and jamming. Reactive security mechanisms, as intrusion detection systems (IDS), are based on network behavior analysis, or previously known attack patterns, being inflexible to handle unpredictable misbehaviors. Furthermore, since new communication technologies are more dynamic and adaptive, attacks are also becoming smarter, often bypassing common security mechanisms [4].

This paper presents a cooperative spectrum sensing framework to effectively provide resilience against both faults and attacks. Applying a low-cost multi-criteria analysis technique, the framework is adaptable to radio environment and flexible to consider unpredictable behaviors that emerge from various practical deployment scenarios. Also, it is able to handle multi-dimensional (e.g. frequency, time, geographical space, security) data in order to effectively sense the spectrum, and detect or mitigate faults and attacks in an optimal way. In the framework, CRs share their initial estimation of the likelihood of an attack with neighbors to gather a collective perception of the network. Thus, they apply the non-parametric Bayesian inference technique to classify spectrum holes and indicate the ones that are least susceptible to failures and attacks, being then resilient in the sense that nodes do not simply rely on majority voting by a collection of nearby nodes. Our approach is evaluated under network disconnections and PUE attacks, considering different sets of physical layer features and their corresponding thresholds that indicate a deviation from the expected results. Simulation results, founded on real traces, show the benefit of the proposed framework in terms of attack detection and its adaptation to network conditions.

This paper proceeds as follows: Section II discusses related works. Section III details the system model and the network architecture. Section IV describes the cooperative spectrum sensing proposed method. Section V presents simulation setup and results for the cooperative spectrum sensing evaluation. Section VI concludes the paper and highlights future works.

II. Related Work

Works in the literature plan to prevent, detect or mitigate attacks in cooperative spectrum sensing for CRNs [4], [5], [6]. In general, they focus mainly on network architectural aspects, such as the existence or not of a central entity, and, hence, result in restricted solutions. Those proposals have evolved from centralized to decentralized and from non-cooperative to cooperative designs.

PUE attacks are a particular challenge for CRNs, being impossible to handle them only by traditional security

978-1-4577-1348-4/13/$31.00 ©2013 IEEE

mechanisms. In these attacks, malicious or selfish secondary nodes pretend PU activities, taking advantage on spectrum access. Chen and Park firstly introduced PUE attacks in the literature [7] and, in their works, authors proposed a "transmitter verification procedure" to distinguish incumbent signals from emulated signals. The proposed scheme defines PUs as UHF TV towers with known locations, and that transmission power of PUs is several orders of magnitude higher than the transmission power of attackers. However, they employ a mono-criterion, the received signal strength, to infer distance and analyze the presence of a PUE in the CRN. As in [7], other works have employed a unique criterion to analyze the presence of PUE attacks [8], [9].

Chen *et al*. [10] discuss the PUE attacks in the context of mobile CR networks, where PUs are wireless microphones. They emphasize that the detection criteria employed by prior works are not meaningful for that type of networks because the properties of the microphones-based networks i.e., low transmission power and mobility. Hence, they proposed the first method to combine two kind of criteria, as RF signals and acoustic information.

Although existing security proposals represent relevant landmarks for security progress in CRNs, another important aspect has been left behind: flexibility to consider different and unpredictable attacker's behaviors and to handle on-the-fly changes in attacker's action or network conditions. The majority of existing proposals are intrinsically tied to predefined criteria, implying that the addition of new ones requires the design of a different solution. Differently from recent proposals, our novel method provides flexibility to consider multi-dimensional criteria for achieving resilience in cooperative spectrum sensing.

III. Network Architecture

We consider an infrastructure-less CR network that has no centralized network entity, and secondary users (CR nodes) communicating among themselves in a multihop and decentralized fashion. A set of CRs ($\mathcal{N}_\mathcal{S}$) is co-located in the presence of a set PUs ($\mathcal{N}_{\mathcal{PU}}$) in the network. From $\mathcal{N}_\mathcal{S}$, a subset $\mathcal{N}_{\mathcal{SL}}$ is composed of legitimate secondary users, and a subset $\mathcal{N}_{\mathcal{SB}}$, i.e. $\mathcal{N}_\mathcal{S} - \mathcal{N}_{\mathcal{SL}}$, is composed of misbehaving CR nodes (also referred to as attackers). Each CR node, n_i, performs measurements on radio environments and processes them individually. In order to keep low the overhead generated by communication among nodes, neighbors exchange preprocessed probabilities.

We assume that CRs have no knowledge on primary users' signal. All CRs use energy detection based sensing, which is a well adopted, simple technique with low computational and implementation complexities [2]. Primary users' signal is detected by comparing the output of the energy detector with a threshold which depends on the noise floor [2].

From the perspective of a legitimate CR node $n_i \in \mathcal{N}_{\mathcal{SL}}$, the strength of a signal it senses from an arbitrary node $n_j \in \mathcal{N}_\mathcal{S} - \{n_i\}$, at the instant t, is denoted by $P_R^{ji}(t)$. The transmission power of a node n_j is denoted by $P_T^j(t)$ and the Euclidean distance between nodes n_i and n_j is denoted by $d^{ij}(t)$. Hence, based on the energy detector signal approach, spectrum sensing is modeled by a binary hyphotesis-testing problem (Eq. 1).

$$H = \begin{cases} H_0 : y_i(t) = & \eta(t), \\ H_1 : y_i(t) = & P_R^{ji}(t) + \eta(t) \end{cases} \quad (1)$$

In the sensing method, the hypothesis H_0 takes place when no transmission is sensed in the spectrum, i.e. $P_R^{ji}(t) = 0$. The hypothesis H_1 expresses the use of licensed spectrum by node n_j. In this case, the power $y_i(t)$ perceived by n_i at the instant t is $P_R^{ji}(t)$ plus signal received from other sources that, in this case, is represented by the thermal noise $\eta(t)$. We assume $\eta(t)$ is the additive white Gaussian noise (AWGN).

In turn, $P_R^{ji}(t)$ depends on $P_T^j(t)$, $d^{ij}(t)$ and on the radio propagation model (Eq. 2). In particular, we assume the Free-Space model for the signal sensed by n_i, if $n_j \in \mathcal{N}_\mathcal{P}$ (e.g. typically high TV tower); in turn, the Two-ray ground model takes place, if $n_j \in \mathcal{N}_\mathcal{S}$, being either a misbehavior or legitimate SU ([11], [12]). G_p^2 and G_s^2 represent the shadowing loss factor in each aforementioned model, respectively.

$$P_R^{ji}(t) = \begin{cases} P_T^j(t)(d^{ij}(t))^{-2} G_j^2, \text{ if } n_j \in \mathcal{N}_\mathcal{P} \\ P_T^j(t)(d^{ij}(t))^{-4} G_j^2, \text{ if } n_j \in \mathcal{N}_\mathcal{S} \end{cases} \quad (2)$$

We assume the presence of a common control channel for information exchange. Thus, data is always reliably exchanged between the nodes, though the content of that data can be erroneous of simply intentionally incorrect.

IV. Cooperative Spectrum Sensing Method

This section presents IMCA, a cooperat**I**ve and **M**ulti-criteria framework for spectrum sensing on **C**ognitive r**A**dio networks. This novel framework effectively provides resilience against both faults and attacks, without differentiating their behaviors. It applies a low-cost multi-criteria analysis technique and is adaptable to radio environment, easily considering unpredictable behaviors that emerge from intelligent attacks. IMCA handles multi-dimensional data in order to optimally and accurately sense the spectrum, detect legitimate PU presence or mitigate faults and attacks effects.

The framework is composed of individual and cooperation phases, referred to as A and B, respectively. Fig. 1 illustrates the individual phase, in which each SU calculates a preliminary probability about the presence of a legitimate PU in the spectrum band, faults and attacks. In phase A, each SU periodically samples multi-dimensional criteria, e.g. received signal strength, distance from PU, transmission power, signal to noise ratio (SNR), noise, transmission rate and other, and calculates the preliminary probability employing NAWUF, a low-cost Normalized Weighted Additive Utility Function broadly applied on various domains [13]. Then, SU shares such probability to its neighbors and waits for neighbor's preliminary probabilities during a short interval of time before starting the phase B. No synchronization among SUs is required, i.e., each node works individually and can ajust its behavior depending on the collected data.

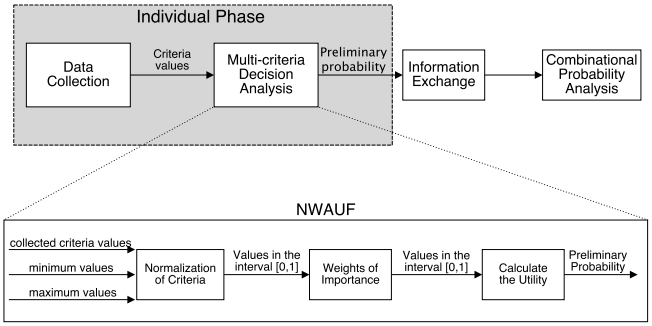


Fig. 1: Phase A: Individual analysis

Fig. 2 illustrates the cooperative phase of IMCA. Each SU starts a non-parametric Bayesian inference having as input the preliminary probabilities received from neighboring nodes and the preliminary probability calculated by itself. The Bayesian inference yields a final probability about the presence of legitimate PUs, faults or attacks in spectrum bands. Final probability can be employed by the phases of the cognitive cycle in CRN, as spectrum decision, spectrum mobility and spectrum sharing, leading their functions.

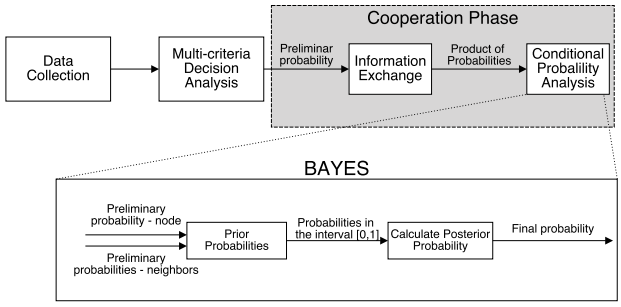


Fig. 2: Phase B: Cooperation

Phases A and B happen periodically in intervals of Δ time. Table I summarizes the notation used to describe the phases of the cooperative spectrum sensing method. From the perspective of a given node n_i, $P_{n_i}(A)$ denotes its preliminary probability, calculated by the phase A. From the perspective of n_i, $P_{n_j}(B)$ and $P_{n_j}(B|A)$ stands for the preliminary and final probabilities of an arbitrary neighbor n_j. Finally, n_i employs the Bayes theorem to infer the final probability $P_{n_i}(A|B)$, considering $P_{n_i}(A)$, $P_{n_j}(B)$ and $P_{n_j}(B|A)$. Next subsections detail individual and cooperation phases of IMCA. We explain the phases considering their execution on a period Δ, however those procedures continue.

A. Individual phase

The first phase characterizes the measurement and the analysis of multi-dimensional criteria to define spectrum sensing conditions. At every time instant t, nodes in N_S take a scalar measurement d_{cz} of some random process δ_c, such as node transmissions, signal reception, noise and other. Each d_{cz} composes the subset $\mathcal{S}_c$, and all subsets $\mathcal{S}_c$, for $c = \{c_1, c_2, c_3, ..., |\mathcal{C}|\}$, form the set of total samples $\mathcal{S}$. During a Δ interval, each criterion owns $z = \{1, 2, 3, ...|\mathcal{S}_c|\}$ data collected from the network, being $|\mathcal{S}_c|$ equal for all criteria. All collected data are organized in a matrix D with z colunms and c lines. Each given CR node n_i in the network will use its matrix D to calculate its individual and preliminary probability $P_{n_i}(A)$ of existing PU activities, faults or attacks in the spectrum band.

TABLE I: Notation

Notation	Definition
$\mathcal{N}_{\mathcal{PU}}$	Set of primary users
$\mathcal{N}_{\mathcal{SL}}$	Set of legitimate secondary users
$\mathcal{N}_{\mathcal{SB}}$	Set of attackers
$\mathcal{N}_{\mathcal{S}} = \mathcal{N}_{\mathcal{SL}} \cup \mathcal{N}_{\mathcal{SB}}$	Set of all secondary users (SUs)
$n_i \in \mathcal{N}_{\mathcal{SL}}$	A given secondary user
$n_j \in \mathcal{N}_{\mathcal{SL}}$	A given neighbor of n_i
$P_{n_i}(A)$	Preliminary probability calculated by n_i
$P_{n_j}(B)$	Preliminary probability calculated by n_j
$P_{n_i}(A\|B)$	Final probability calculated by n_i
$P_{n_j}(B\|A)$	Final probability calculated by n_j
$\mathcal{C}$	Set of criteria
$\mathcal{S}$	Set of samples for all criteria
$\mathcal{S}_c$	Set of samples for a criteria c
W	1 x $\|\mathcal{S}\|$ vector of criteria weights
MIN	1 x $\|\mathcal{S}\|$ vector minimum values for criteria
MAX	1 x $\|\mathcal{S}\|$ vector of maximum values for criteria

IMCA applies criteria from different dimensions, such as time, frequency, geographical position, security mechanism, layer of the protocol stack and other, in order to accurately sense the spectrum and detect attacks or failures. Since data collected from these varios dimensions are not homogeneous, IMCA employs NWAUF to perform their analysis. NWAUF consists in a multiple-criteria decision analysis (MCDA) technique, based on normalized criteria values and weights of importance ranging from 0 to 1, with a culmulative sum of one. The 1 x $|\mathcal{C}|$ vector W contains the weights for each employed criterion. Then, W =$\{w_1, w_2, \ldots, w_{|\mathcal{C}|} \mid \sum_{c=1}^{|\mathcal{C}|} w_c = 1\}$. NWAUF follows four well defined steps: i) identifying criteria values; ii) normalizing values; iii) assessing weights of importance; iv) calculating utility function values.

i) Identifying criteria values: After measuring criteria during a Δ interval, NWAUF defines the maximum and minimum values per criterion based on the amount $|\mathcal{S}_c|$ of collected samples. Two 1 x $|\mathcal{S}_c|$ vectors, MIN and MAX, store respectively the minimum and maximum values per criterion.

ii) Normalizing criteria values: Based on the MIN and MAX vectors, NAWUF normalizes collected samples into the range from 0 to 1, following Eq. 3 (illustrated for a scalar measurement).

$$\overline{d_{cz}} \leftarrow \frac{d_{cz} - MIN_c}{MAX_c - MIN_c} \forall c \in \mathcal{C}; z \in \mathcal{S}_c \tag{3}$$

iii) Assessing weights of importance: The important step in the NAWUF probability calculation lies in defining the weights associated to each criterion. IMCA defines the weights by means of the Principal Component Analysis (PCA) statistical procedure [14]. However, any other technique could be

applied. PCA estimates the values for criteria weights, i.e. W, by means of a weighted sum of parameter values. PCA produces a set of components $y_1, y_2, \ldots, y_{|\mathcal{C}|}$ from the set of criteria $\mathcal{C}$ in which each y_i is called the principal factor. Each y_i explains a percentage of the variance among criteria, i.e., defines values for $w_1, w_2, w_3, ...w_{|\mathcal{C}|}$.

iv) Calculating utility: The preliminary probability $P_{n_i}(A)$ is calculated in this phase of NWAUF as an utility function. Calculation follows Eq. 4, where the sum of weights is employed in conjunction with normalized criteria values.

$$P_{n_i}(A) \leftarrow P_{n_i}(A) + W_c \cdot \overline{d_{cz}} | \forall c \in \mathcal{C}; z = 1 \rightarrow |\mathcal{S}_c| \quad (4)$$

Algorithm 1 presents the steps for the preliminary probability calculation in the individual phase.

Algorithm 1 NWAUF Analysis

```
1: procedure NWAUFANALYSIS(C, D, W, MIN, MAX)
2:     P_{n_i}(A) ← 0;
3:     for all c ∈ C do
4:         for all z = 1 → |S_c| do
5:             d_cz ← (d_cz − MIN_z) / (MAX_z − MIN_z);
6:             P_{n_i}(A) ← P_{n_i}(A) + W_c · d_cz;
7:         end for
8:     end for
9: end procedure
```

B. Cooperation

The phase B is characterized by the cooperation among nodes, i.e. the exchange of preliminary probabilities between pair of neighbor nodes. From the perspective of a node n_i, the phase B starts when it receives the preliminary probability calculated and shared by its neighbors. The method considers the preliminary probability $P_{n_j}(B)$ calculated and shared by the j-th neighbor of n_i to update the initial estimative $P_{n_i}(A)$ of the n_i, i.e. to calculate the final probability $P_{n_i}(A|B)$ about the presence of attacks or failures in the network.

A given SU node n_i performs a non-parametric Bayesian inference (Eq. 5) to calculate $P_{n_i}(A|B)$ based on probability values received from at least k neighbors. The Bayes theorem requires, in its first execution round, a previous estimation or mesurement of the neighbors final probabilities. Thus, for the estimation of the *first* final probability $P_{n_i}(A|B)$ of a given node n_i, the method assumes constant value α as neighbors' final probabilities. Note from Eq. 5 that this makes the first estimation of the type $P(A|B)$ to be only influenced by values taken from measurements, i.e. the values of $P_{n_i}(A)$ and $P_{n_j}(B)$. Hence, the probabilities of the type $P(B|A)$ will be known after the first round of the scheme by means of the probability exchange among nodes.

$$P_{n_i}(A|B) = \frac{P_{n_i}(A).P_{n_1}(B|A)}{[\sum_{j=1}^{k} P_{n_j}(B).P_{n_j}(B|A)]} \quad (5)$$

Fig. 2 highlights the steps performed by each SU node in the cooperation phase, in which a conditional probability analysis occurs to determine the probability of the presence of attacks or failures in the network.

V. Evaluations

This section presents the performance evaluation of IMCA, the proposed cooperative spectrum sensing framework employed to improve resilience of cognitive radio ad hoc networks. In order to show the multi-dimensional feature of IMCA, evaluations are performed under two different combinations of the following criteria, calles as cases 1 and 2: *received signal strength*, *transmission power*, *distance*, *noise* and *transmission rate*. In **case 1**, we employ a combination of *received signal strength*, *distance* and *transmission power* criteria; whereas **case 2** employs *received signal strength*, *Signal to Noise Ration (SNR)*, *noise* and *transmission rate*. However, other criteria could be added to the cases. These criteria have been chosen due to their importance in the literature. Next subsections describe the evaluation scenarios, results and analyses.

A. Performance Evaluation Setup

Our simulations are performed in the Network Simulator (NS), version 2.31, using the modules for cognitive radio ad hoc networks developed by Di Felice et al. [15] with the parameters described in Table II.

TABLE II: Simulation parameters values

Simulation Parameter	Value
Secundary users (SUs)	50
Primary users (PUs)	2
Rate of PUE attackers	10%, 30%, 50%
Number of channels	11
Simulation time	500 seconds
SUs transmission range	250 m
PUs transmission range	1000 m
Attacker transmission range	250 to 1000 m
SUs transmission power	24.5 dBm
PUs transmission power	94 dBm
Attacker transmission power	24.5 to 94 dBm
Routing protocol	AODV
Area	1000x1000 m

Our simulations are composed of $|N_{PU}| = 2$ and $|N_S| = 50$ static nodes. We vary $|N_{SL}|$ and $|N_{SB}|$ to represent different rate of PUE attackers in the network. There are $|M| = 11$ licensed channels available in the network. We assume both PUs and nodes in N_{SB} accessing and attacking a given channel following a random uniform distribution. With no loss of generality, particularly for the performance case studies, the geographical position of a transmitter $p_1 \in N_P$ is publicly known (e.g. a TV tower) and any static node $n_i \in N_{SL}$ can infer its distance $d^{ip_1}(t)$ from p_1. The transmission power $P_T^{p_1}(t)$ of p_1 can be known from its underlying PHY standard.

We compare results based on the probability Pr of the presence of a PUE attack in the network over an increasing rate of attackers. Since the evaluated framework is cooperative and resilient, we compare both cases considering Pr taken by analyzing the improvement achieved by the individual and cooperative phases.

Further, we also measure the detection rate $T_{k,i}$ of the node $n_i \in N_{SL}$ for different number k of cooperating neighbors in order to evaluate the resilience of the framework. $T_{k,i}$ is given by $T_i = \frac{\sum_{j=1}^{k} P_{n_j}(A|B)}{k}$, in which $P_{n_j}(A|B)$ is the individual probability shared by the j-th neighbor of n_i and $0 \leq k \leq |N_{SL}| = |\{n_i\}|$ is the corresponding to cooperating neighbors and emulating faults in the network connectivity.

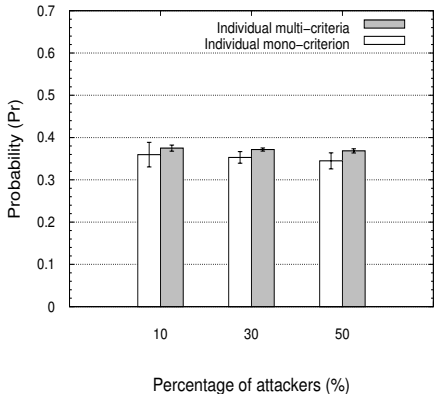
In order to emphasize the importance of well-defining weights, in case 2, PCA uses as input samples from real cenarios available in the CRAWDAD (Community Resource for Archiving Wireless Data At Dartmouth) data repository. Since criteria are independent from the communication technology, experimental scenarios in CRAWDAD employed 802.11g and 802.11a in a total of 10 nodes with a transmission power of 15 dBm and transmission rate of 11 Mbps and 13 nodes with transmission power of 15 dBm and transmission rate of 6Mbps. Samples are normalized and after a matrix of criteria correlation is yielded in order to calculate the weights by PCA. The R tool was employed to calculate the weights of importance employed in case 2. Hence, weights of 0.45, 0.25, 0.18 and 0.12 are applied in case 2 for, respectively, the following criteria: *received signal strength*, *SNR*, *noise* and *transmission rate*.

For case 1, PCA was also employed, however inputs are provided by simulationsin NS-2. The following weights of importance are employed for case 1: 0.45, 0.29 and 0.26 considering, respectively, reception *received signal strength*, *distance* and *transmission power*. Results also compare achievements for both cases and for a situation where PCA was not employed, in order to highlight the importance of well-defining weights. Results from both cases and from a scenario where no PCA is employed have been compared with results achieved by a generic mono-criterion approach, i.e., a distributed cooperative approach applying received signal strength criterion for analyzing spectrum band conditions representative of the literature. For both approaches (multi-criteria and mono-criterion), we report and analyze results.

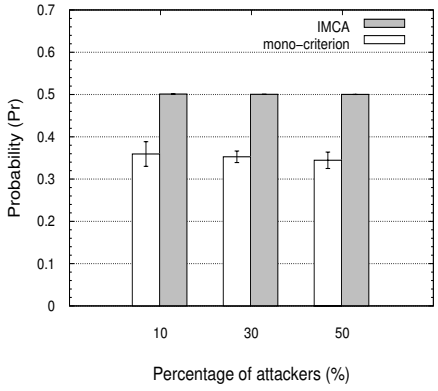
B. Results and analysis

Figs. 3 (a) and 3 (b) compare case 1 with the mono-criterion approach when no PCA analysis is employed. Instead, we assigned 50% of relevance to the received signal strength criterion based on the fact that it has been the single criterion adopted in the state of the art, as aforementioned. For this case, we assigned 25% for the weights of each other two criteria. From Figs. 3 (a) and 3 (b), one can observe that the individual multi-criteria approach (i.e., the method before cooperation) slightly outperforms the mono-criterion approach as the rate of attackers increase over 10%, 30% and 50%. These improvements correspond to 1.53%, 1.85% and 2.36%, respectively. When cooperation takes place, the improvements are more expressive: about 15.56% for all rates of PUE attacks.

Similarly, Figs. 4 (a) and 4 (b) compare cases 1 and 2 of the scheme with the mono-criterion approach. Weights are defined in a off-line way according to the previously explained PCA analysis using realistic data available at [16]. Under the defined



(a) Only individual phase



(b) Both phases

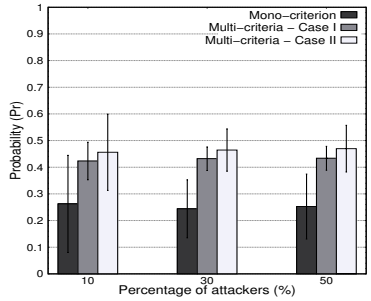
Fig. 3: Individual and cooperation phases without PCA

weights, improvements due to the scheme are even higher for both individual and cooperative phases. Case 1 outperforms the mono-criteria approach by 16%, 19% and 18%, respectively; whereas case 2 presents an improvement of 19%, 22% and 25%, respectively. In case 2, the definition of weights worked together with the cooperation phase to improve the detection of attack and failures in the network. The gains of the scheme over the mono-criterion approach are up to 77% and 73% for the cases 1 and 2, respectively.

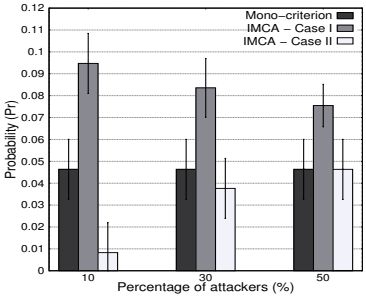
Taken together, our results suggest not only the relevance of the node cooperation, but also *what* is being shared in the cooperation process. In fact, when the information shared by cooperating neighbors account multi-criteria, the benefit due to cooperation for detecting PUEAs can be improved (Fig. 5). However, for a number of cooperating neighbors higher than 3, we observed no difference in detection rate, reinforcing the resilience aspect of the proposed framework.

VI. Conclusion and Future Works

In this work, we presented IMCA, a cooperat**I**ve and **M**ulti-criteria framework for spectrum sensing on **C**ognitive radio **A**d hoc networks. This novel approach effectively provides resilience against both faults and attacks, without differentiating their behaviors. It applies a low-cost multi-criteria analysis technique and is adaptable to radio environment,



(a) Only individual phase



(b) Both phases

Fig. 4: Individual and cooperation phases with PCA

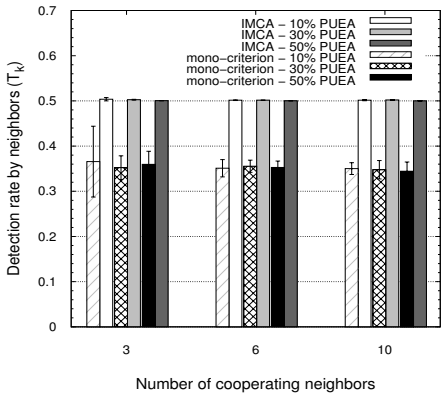


Fig. 5: Number of cooperating nodes

easily considering unpredictable behaviors that emerge from intelligent attacks. IMCA handles multi-dimensional data in order to sense the spectrum, detect legitimate PU presence or mitigate faults and attacks effects. We evaluate IMCA considering scenarios relevant for the literature and tunned based on real traces from the CRAWDAD data base repository. Simulation results show that the proposed method significantly outperforms a mono-criterion approach. As future work, we intend to analyze also the performance and computational cost for the on-line adaptation of weights employed by IMCA.

REFERENCES

[1] E. Axell, G. Leus, E. Larsson, and H. Poor, "Spectrum sensing for cognitive radio : State-of-the-art and recent advances," *IEEE Signal Process. Mag.*, vol. 29, no. 3, pp. 101 –116, 2012.

[2] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116 –130, 2009.

[3] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: a survey," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1691 – 1708, 2012.

[4] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 355–379, 2012.

[5] L. Duan, A. Min, J. Huang, and K. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE J. Sel. Areas Commun*, vol. 30, no. 9, pp. 1658–1665, 2012.

[6] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Commun.*, vol. 19, no. 6, pp. 106–112, 2012.

[7] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun*, vol. 26, no. 1, pp. 25–37, 2008.

[8] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *IEEE ICC*, 2009, pp. 2749–2753.

[9] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics," *IEEE Trans. on Wireless Comm.*, vol. 9, no. 11, pp. 3566 –3577, 2010.

[10] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is believing: Detecting mobile primary user emulation attack in white space," in *IEEE INFOCOM*, 2011, pp. 36 –40.

[11] S. A. Z. Jin and K. P. Subbalakshmi, "Neat: A neighbor assisted spectrum decision protocol for resilience against primary user emulation attacks," *Technical Report*, 2010.

[12] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *IEEE DySPAN*, 2008, pp. 1–6.

[13] W. Ho, X. Xu, and P. K. Dey, "Multi-criteria decision making approaches for supplier evaluation and selection: A literature review," *European Journal of Operational Research*, vol. 202, no. 1, pp. 16 – 24, 2010.

[14] R. Jain, *The Art of Computer Systems Performance Analysis*, 1st ed. John Wiley and Sons, 1991.

[15] M. D. Felice, K. Chowdhury, W. Kim, A. Kassler, and L. Bononi, "End-to-end protocols for cognitive radio ad hoc networks: An evaluation study," *Performance Evaluation*, vol. 68, no. 9, pp. 859 – 875, 2011.

[16] CRAWDAD, "Community Resource for Archiving Wireless Data At Dartmouth," Last access: Sep. 2012, http://crawdad.cs.dartmouth.edu/.