IDS-COG - Intrusion Detection System for Cognitive Radio Network

Joffre Gavinho Filho†, Luiz F. R. C. Carmo††, Raphael Machado†† and Luci Pirmez†

† NCE/IM, Federal University of Rio de Janeiro, Postal Code 2324, Rio de Janeiro, RJ, 20001-970 – Brazil
†† Inmetro, Duque de Caxias, RJ -25250-020 - Brazil

Summary
An Intrusion Detection System (IDS) for Cognitive Radio Network (CRN) is proposed. The considered IDS is constructed by combining two classic mechanisms for CRN intrusion detection, namely the Localization mechanism and the Reputation mechanism. The composition of the mechanisms is done with the aid of a Genetic Algorithm (GA) responsible for calibrating the IDS, that is, for attributing "weights" to each of the mechanisms. Simulations have been implemented that demonstrate a superior performance of our proposal, when compared to an uncalibated IDS

Key words:
Cognitive Radio Network, Intrusion Detection System, Security

1. Introduction

Recent measurements of the spectrum [16] demonstrate that the spectrum's static allocation policies are improper for the current wireless communications scenario. According to the report of the Federal Commission of Communications (FCC) [6], the majority of the attributed spectrum bands (licensed frequency bands) are not used in certain periods of time or in certain geographic areas, causing the called "white space", while the permitted frequency bands are always congested. A possible way to solve the problems of underutilized permitted bands and the limited availability in permitted bands is not allowing that non permitted users, called secondary users (SU), have dynamic access to the permitted bands, since they do not provoke interference with the proprietors of the permitted bands, called primary users (PU). In this context, the Cognitive Radios (CR's) are presented [15], as a promising concept, which allows dynamic access to the radio frequency spectrum [1]. In a network formed by CR's, the devices possess flexibility in the access of the spectrum, with capacity to detect the available bands, to reconfigure the radio frequency, and to exchange between the selected bands [1]; on the basis of the sensing information of the spectrum, the CR users opportunistically access the permitted bands when no PU uses them, and, necessarily, they must immediately leave them when detecting activity of the PU. On the other hand, the use of the CR's technology brings benefits as to: (i) solve the problem of scarcity of available frequencies in the radio frequency spectrum; (ii) improve the potential performance of wireless communications; (iii) minimize the interference between radio devices. The CR technology also originates a series of challenges that still must be surpassed, propitiating a vast field for research. Among the challenges to be explored in the CR field resides the challenge of providing security to the Cognitive Radio Network (CRN), since the equipment used in such networks can be victim of actions that can stop their communications, as the Denial of Service (DoS), for instance. Thus, in a CRN, an attacker, using "a malicious" transmission, can induce the CR's to interpret that the permitted bands, that could be used by them, are in use. In short, such actions can degrade partially, or totally the CRN operation. In the present work, an Intrusion Detection System (IDS) is designed for a CRN For the conception of the IDS, reputation and localization mechanisms had been investigated. The localization mechanism (LM) of malicious users in the network will make possible the determination of the radios geographical positioning. This mechanism associated with the transmission power levels of each radio will identify if the analyzed radio is a PU, or a SU. Such mechanisms were already considered in [18] and [4] by means of the insertion of a wireless sensor network (WSN), secondary to the CRN, where the necessary analyses and calculations to the viability of the LM were carried through. In the present work, we present an extension to the concepts displayed in [18] and [4], once the proper participant radios of the network are responsible for supplying the data on which the localization algorithms will be executed. Such improvement, in one hand, excludes the necessity of a WSN. On the other hand, mechanisms are necessary to validate the confidence of the data supplied for the radios,

Manuscript received March 5, 2012
Manuscript revised March 20, 2012

what it is made by the Reputation Mechanism (RM). The use of the reputation mechanism attributes a "degree of acceptance" to an individual of the CRN to communicate without requiring the radio to have previously interacted with the target CR and, in such a way, it uses the experiences of the CRN. While the works cited above investigated detection mechanisms in an isolated way, in the present work we opted to consider an IDS based on the joint use of the localization methods and on the reputation system. Such choice for the conception of an IDS based on the two cited methods has three main reasons: (i) to group in an unique IDS the detection of different attacks; (ii) to increase the robustness of the IDS, and, finally; (iii) to optimize the detection system. Thanks to the joint use of the LM and RM, the proposed IDS will be capable to detect attacks of Primary User Emulation (PUE) and of Spectrum Sense False Feedback (SSFF). These Attacks were chosen for being the two main CRN attack types [12]. The two methods will be grouped into only one, then having the necessity of the attribution of weights for each one. This attribution is made necessary because each set of solutions can have a bigger or smaller influence in relation to another data set in what it says respect to the convergence of the mechanism in the classification of the intrusion. The concept of Genetic Algorithm (GA) [11] for the attribution of weighed weights to each one of the mechanisms will be used.

This article is organized in five sections. Section 2 presents the basic concepts of this work and Section 3 the related works. In Section 4 the experiments and the analysis of its results are described. Finally, Section 5 contains the conclusions.

2. Theoretical Consideration

An attack in a CRN is defined successful when it reaches one of the following objectives [12]: (**i**) **unacceptable interference to the PU** - a SU verifying that a permitted transmission started its process of communication in one determined frequency band, and not to interrupt, or to initiate, a transmission in this same band - reducing, or making unusable, for consequence, the communication capacity of the PU; (**ii**) **use blockage of the free permitted frequencies** - the attacker occupies maliciously the permitted channels of the spectrum, hindering their occupation by the SU, causing the DoS in the CRN and; (**iii) injection of false data** - provoking the execution of unexpected actions by the radios. It is found in literature the specification of the variety of new attacks to the CRN, which we cite: (**i**) **Spectrum Sense False Feedback - SSFF**. The detection of the spectrum is the basic characteristic of the CR, functionality that can be carried through by a radio, or for all network. When the detection will be carried, all the pertaining notarized radios of the CRN, in some moments, have the function to receive the information of the availability of the free permitted channels from the other radios. They are called data fusion centers (DFC), which are responsible for processing and informing the CRN about the table of free frequencies. However, an attacker or a malicious user, or someone with bad functioning, can emit false information on the local spectrum. As an example, informing to the data fusion center that a certain frequency is being used for the main user, when in fact the frequency is free. The DFC processes and consequently disseminates the tables of permitted frequencies with wrong values [17]. Classifying SSFF according to the quantity of fake information in the sensing spectrum , we will find three distinct types of attacks: (**a**) **always-free - SSFF-AFr** - the frequency of the PU is busy but it is informed as free ; (**b**) **always busy - SSFF-AB** - the frequency is free, but it is informed as busy, and; (**c**) **always false - SSFF-AFa**- the information presents the inverse of the reality - free when it is busy and busy when it is free [27]; (**ii**) **Primary User Emulation Attack - PUE**. In view of [18], it is the attack where a malicious radio tries to impersonate the figure of the PU, transmitting in the free bands in the periods where the CRs could use them, causing with this the DoS in the secondary network. When the PUE attack is used for a "selfish" possession of the permitted frequency spectrum, it is called of **Selfish PUE – PUE-S**. When such attack has the only purpose of blocking the free channels hiding its use from parts of the CRN, it is called **Malicious PUE – PUE-M**.

2.1 Localization Mechanism

Many proposals had been presented in the context of CRN security [4], [5], [12] that use as detection method of PUE attacks the use of the localization of the SU and the PU. The chosen proposal as base mechanism for the present work is focused in [18]. In order to deal with the PUE attack, the authors proposed in [18]: the use of the detection of the energy level of the signals received to find the localization of the transmitters as following: (i) the primary transmitters are TV towers with a fixed known position; (ii) the CR is a device with limited power of transmission (it varies from *miliwatts* - mW – to some watts - W). As consequence, the detection of the energy level can, definitively, be a robust criteria to validate the authenticity of primary transmissions. An approach is to verify if data signals are from the main transmitter; esteem its position and to observe its transmission characteristics. In order to esteem the position of the signal transmitter, a non interactive localization approach is used, that is, it does not have any interaction of the SU with the PU. The localization of the signal of the primary transmitter was

defined as non interactive in virtue of two basic premises of the CR paradigm: (i) no modification to the PU to accommodate the new technology, and, in result of this; (ii) it cannot have any type of interaction between the CRs and the PU. A localization approach must then be used, which does not carry through any type of communication between both users. The LM collects in real time the Received Signal Strength (RSS), being the RSS nothing more than the measurement of power of the received signal. The verification approach of the transmitter includes three stages: (i) verification of the signal characteristics; (ii) measurement of the energy level from the signal received; and (iii) the localization of the signal source. The basic idea of the considered localization system uses the fact that the RSS value diminishes as the distance between the signal transmitter and receiver increases [9]. The statistical model used to shape the propagation behavior of the signal can be found in [19], however, to adapt the scenario for great cities and frequencies above of 400 MHz, in the present work we use [8], as follows:

$$\Pr = \frac{Pt * Gr * Gt}{L} \quad (1)$$

$$L = 69{,}55 + 26{,}16\ell og(f_{mhz}) - 13{,}82\ell og(h_{Tef}) - a(h_{\mathrm{Re}\,f}) + [44{,}9 - 6{,}55\ell og(h_{Tef})]\ell og(d_{km}) \quad (2)$$

$$a(h_{\mathrm{Re}\,f}) = 3{,}2[\ell og(11{,}75h_{\mathrm{Re}\,f})]^2 - 4{,}97) \quad (3)$$

Where: In Equation 1: ***Pt*** and $\mathbf{P_R}$ are of the strength of transmission and reception (in Watts); $\boldsymbol{G_T}$ and $\boldsymbol{G_R}$. are the gains of the transmitter and receiver antennas, respectively, e; ***L*** is the loss in the transmission, and; in Equations 2 and 3: ***f*** is the frequency of 150 the 1500 MHz; ***d*** is in the distance, varying from 1 to 20 km; $\boldsymbol{h_{Tef}}$ is the height of the transmitter antenna (where the antenna is positioned), varying from 30 to 200 m; $\boldsymbol{h_{Ref}}$ is the height of the receiving antenna, varying from 1 to 10 m, and $a(\boldsymbol{h_{Ref}})$ it is the factor of correction of the height accomplishes of the receiving. After the analysis of the RSS, the calculation of the positioning of the SU supplies a extremely robust way to identify of radios participating of an attack of PUE,

2.2 Reputation Mechanism

In the RM, we verify that the specialized literature [7], [14], [20], [26] uses as reference mechanisms to classify the reputation,the information the collaborative and cooperative sensing of the permitted free frequencies. On the basis above displayed, we define as the source of our mechanism, part of the work considered in [27], which has, as focus, to identify SSFF attacks [12]. Such identification is carried through the analysis and weighted classification of the reputation and credibility of the radios on the CRN. The cooperative detection of the spectrum, uses a classic data fusion model [1], it is one of the most efficient methods so that a SU defines which permitted band of the spectrum is free or busy for the transmissions of the PU, so that he can make use, or not, of such bands. The classic data fusion model is formed basically by a DFC, i.e. the radio that receives the information from the radios about the spectrum (Figure 1).

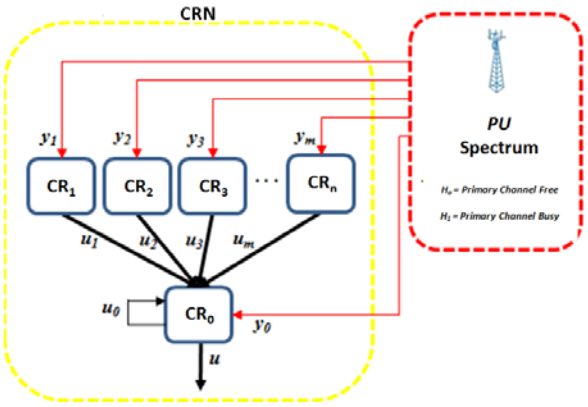


Figure 1. Demonstrates a classic model of fusing of the data.

The fusion center could be any one of the CRs that need to use the free permitted channels in a defined time (Δt). In our example, the data fusion center (DFC) is represented by radio CR_0. The information received by the DFC (CR_0) is defined as u_i, being u_i= 0,1,2,3,… m, from the neighboring CR (CR_i), and to the free permitted channels (H_0), and the channels used byPU transmissions (H_1). Being u_i =0 or u_i =1, the decision of the CR_i is H_0 or H_1 respectively. Such information has as base the perception that each CR_i has its own monitoring of the spectrum, defined as y_i. Each u_i received by CR_0 from CR_i is loaded on the fusion vector V_u. Finally, the DFC, based on the received monitoring information, as well as on the detection of the spectrum, extracts a global decision, u, where u = 1 means the occupation of the permitted channel, that is, H_1, and u = 0 the channel is free, H_0. However, in case some radio, because of a defect, or "acting" maliciously, presents to the fusion center an incorrect detection, it will be able to compromise the functioning of the whole network. Basically, the mechanism makes the analysis of the information u_i and the attribution of weights w to the CR_i. After initializing the system, the credit of each CR_i radio is adjusted to zero, that is, each CR_i can accumulate credits for correct information u_i.

Whenever the information of one determined radio will be consistent with global decision u, that is, the processed final information for the CR_0, its credit will be increased by one; if not, then diminished of one. Denoting the credit for the CRi by Ci, the credit system can be represented as in Equation 4. When increasing the reputation of a radio that has incorrectly classified the detection of the permitted channel, the weight, before being attributed to the CR_i, is normalized by the average of the credits of the CR_i radio.

$$Ci = \begin{cases} Ci + 1, & if \quad u_i = u \\ Ci - 1, & if \quad u_i \neq u \end{cases} \tag{4}$$

$$w_i = \begin{cases} 0, & if \quad Ci < -g \\ \dfrac{Ci + (-g)}{avg(Ci + g)}, & if \quad Ci > -g \end{cases} \tag{5}$$

$$W = \sum_{i=0} (-1)^{ui+1} wi, \tag{6}$$

$$\begin{cases} W \geq q & \rightarrow accept\ H_1 \\ W \leq q & \rightarrow accept\ H_0 \\ -q < W < q & \rightarrow \text{proceed to another analyse} \end{cases}$$

In the above described equation: w_i is the weight of the CR_i, C_i is its respective credit; *avg* (C_i) denotes the average credit of the CR_i, and g is a normalization constant whose value is of 5.51, which was analyzed and calibrated by [23]. The Vector of V_w Credibility is then loaded as the value of w_i for each CR_i. The bring-up test is initialized with the determination of the acceptability threshold q. This threshold is used for the DFC to make the decision on how much of the permitted channels are occupied or not. The Value q is used as superior limit and – q used as inferior limit of the bring-up test. In samples u_i then are taken one to one to execute the sequential test, and the same difference between values 1 and values 0 is finished when equal or exceeding the superior limit or the inferior limit, that is, q or - q, respectively. We can observe that after the analyses carried through in the mechanism the CR_0 will assume u=1 when W≥ q; u=-1 when W≤ q, and; will proceed to another round from analyses when - q < W < q. After the carried through analyses, had the convergence of the credibility for a credibility minimum of those radios whose information of free channels are different from the global decision of each cluster. The Genetic Algorithms (GA's), are, according to [11], optimization methods inspired in the live beings evolution mechanisms and are implemented as a computer simulation where the solution is represented by an abstract representation of the population and it is selected by brainstorming. This mechanism is used to calibrate the proposed IDS.

4. Experiments with the IDS for CRNs

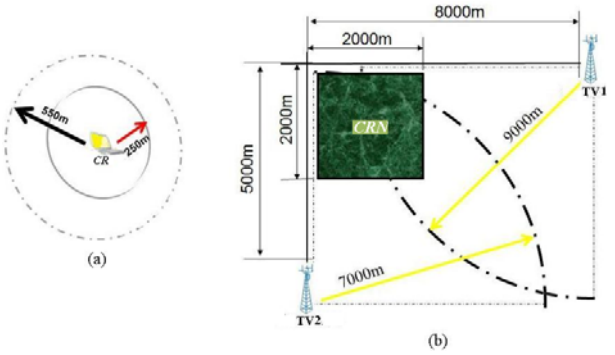
In virtue of the non-existence of a real CRN, and even of physically mounted CR's, we have the necessity of accomplishing the experiments by means of simulations. Four experiments are presented. In the first and second, simulations had been carried through with the intention to calibrate the considered IDS. In the first, we try to determine the most adequate Threshold Value of Acceptability (TVA) of the CRs, as well as the Value of the Normalization Constant (VNC) of the radios credibility, in terms of the number of valid information, or not, on the permitted frequencies. In the second experiment, we try to determine the necessary time for the CRN convergence in terms of: correct detection rate of attacks and in a normal situation, of a way to detect with precision the PUE and SSFF attacks on the part of only one radio. In the third experiment, the transmissions of the PUs and the CRs, as well as the two first stages of the execution flow of the considered IDS (localization and reputation) had been implemented in Matlab/Simulink 7.1® with the objective to evaluate the efficiency of the algorithm. Finally, in the fourth and last experiment, to each detection value calculated in the previous experiments, weights by means of the GA are attributed.

4.1 Description of the scenario, experiments and metrics

For the experiments, a decentralized wireless network with plain topology and fixed nodes was implemented. Considering the physical disposal of the CRN we look to reproduce that one used in [18]. The CRN was composed of 300 CRs, distributed randomly in a square shaped area of 2000m; each CR possesses a transmission radio of 250m, with an interference radio of 550m, following the model considered in [10] (Fig. 1a).

Transmission of the CRs is in 24dBm, possessing antennas with sensitivity of -94dBm, 1m of height, and frequency of transmission at 617MHz. Two PU's (tower of TV 1 and

Tower of TV 2) are located at 8000m and 5000m from the external edges of the CRN (Fig. 1b). The towers possess 84dBm and 83dBm and reach 9000m and 7000m, respectively; frequency of transmission of 617 MHz; using 10 numbered channels from 1 to 10. Each tower possesses a height of 100m.



Used scene: (a) Ray of Reach of the CR. (b) Diagram of CRN

The metrics used to analyze the experiments were [24]: (i) false positives (FP), that indicate the amount of false alarms; (ii) false negatives (FN), that indicate a normality condition when in fact an attack is occurring; (iii) true positives (TP), that indicate that an attack is occurring during an attack in fact; and (iv) true negatives (TN), that indicate a normality condition when no attack is occurring.

4.2 Simulation and Results

The simulation is divided in two stages, each stage consisting of a module: the first module generates the scenario for the simulation, and; as it simultaneously generates the transmissions: of the TV towers, of the CRs and the attackers. When the detection mechanism is executed, fulfilling itself with the calibration of the detection coefficients. In the first stage, the network is composed with the random distribution of the 300 CRs in the CRN. Then, the initialization of the CRN is performed, where each neighboring CR identifies its CRs, that is, those in its reach. Once that the 300 CR's are deployed, each of them is considered as center of a cluster. The calculations are carried through to determine the CRs that are in reach of the transmissions of the Tower of TV1, the Tower of TV2, both, or of none of them. After that, the second stage is initialized, where, simultaneously, there is the simulation of the transmissions of the TV Towers and the CRs, for 1 hour. We define as base time unit 10 ms, which we call a slot. Randomly, some channel is chosen to be occupied in this slot by one of the TV Towers, only one of them, or none. Simultaneously, it is defined how many of CRs will transmit in this slot; each CR defines if it will make a data or control transmission. In the control transmission 1 packet is chosen among 5 packages to be transmitted (each package is equivalent to a slot), while in the transmission of data, it varies of 1 to 10 packages. The CR senses the environment, verifying if the spectrum is occupied (channels) by the PUs (TV Towers), by another neighboring CR, or by some transmission interference. In case that it does not have any problem, the CR transmits 1 package, and in case that it possess more packages to transmit, it waits the next slot to transmit. Simulations with and without attacks are carried through. The simulations with insertions of attacks consist of choosing a CR, and are carried in order to analyze the behavior of the Localization and reputation mechanisms isolated, that is, using the Localization Mechanism only in the detection of PUE attacks, and of Reputation only in the detection of SSFF attacks as well as the combination of the two mechanisms for the detection of the attacks. The simulations with attacks consist, in the case of Attacks of PUE, in the insertion of CRs that, in random instants, occupy a slot vacant and due to a priority use it. And, in the case of the SSFF, has the insertion of CRs in random instants, tables that emit adulterated frequencies. The Localization Mechanism is executed each 1 second, through reception tables of daily pay-configured powers. These tables are initialized through Euclidean calculation of the distances between each CR and its neighbors, as well as between the CRs and the TV Towers. The reception powers then are calculated [7] with a random measurement power varying error from -10% to 10% (uniform rate).

The CRs, that need to transmit, when verifying that it has occupied the spectrum of permitted frequency, and whose characteristics are not fit with the transmission of the neighboring radios, that is, the packages do not contain MAC address (physical address of 48 bits of the station, or, more specifically, of the net interface), goes off the localization mechanism. The power of the signal is analyzed, when the existence or not of PUE attacks is defined. The Reputation Mechanism is executed at each 2.5 second, by means of the analysis of tables of frequency received from the CRs neighboring, as well as of tables of the proper CR that makes the analysis. Through calculations of credibility, attribution and reputation, indices are attributed to the CRs. In case that some CR exceeds the TVA, as it can be observed in the code, this is defined as an attack. The thresholds of upper/lower acceptability (q and - q), have been defined by [27], as 15 and -15, respectively, as well as the VNC g in 5.51. Two Hundred And Ten (210) rounds of simulation have been carried through, being 30 simulations for each one of the following types: without attacks; varying only the attack of PUE Selfish of 1 the 30 attacking radios; varying only the Malicious attack of PUE of 1 the 30 attacking radios; varying only the attack of SSFF-AFr of 1 the 30 attacking

radios; varying only the attack of SSFF-AB of 1 the 30 attacking radios; varying only the attack of SSFF-AFa of 1

(1) Amt.	(2) Type of Attack	(3) CR's transmit	(4) CR's that they had transmitted	(5) Packages to transmit	(6) Packages effectively Transmitted.
0	**Without**	2.691.394	5.267	12.107.175	89.584
1	**PUE S**	2.032.601	5.208	11.359.036	88.688
30	**PUE S**	2.695.563	1.177	12.210.425	66.265
1	**PUE M**	2.128.404	5.311	12.734.860	88.812
30	**PUE M**	2.413.363	226	12.131.096	66.358
1	**SSFF-AFr**	2.572.904	5.018	12.226.692	87.432
30	**SSFF-AFr**	2.768.152	5.199	12.733.963	65.327
1	**SSFF-AB**	2.732.220	5.347	12.116.144	85.163
30	**SSFF-AB**	2.442.436	0	12.738.830	63.631
1	**SSFF-AFa**	2.453.715	5.289	11.181.238	87.771
30	**SSFF-AFa**	2.764.480	835	12.810.070	65.580
5	**All**	2.254.649	5.812	12.039.828	87.904
150	**All**	2.013.124	0	11.970.240	32.888

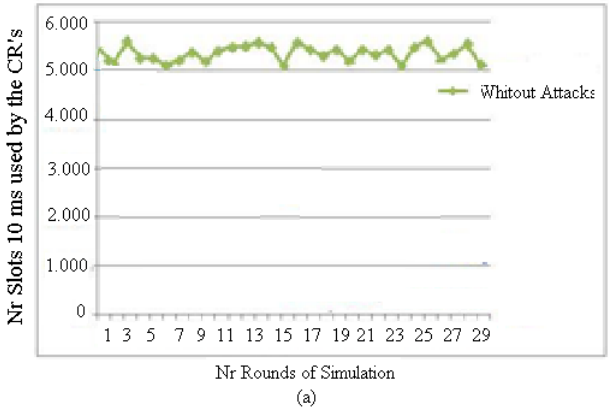
the 30 attacking radios, and finally, varying all the attacks in set of 5 the 150 attacking radios, observing that each CR alone carries through a type of attack.

Table 1 is formed by 4 columns, namely: column 01 (Nr of attackers), amount of attackers simulated in one slot; column 02 indicates the type of transmission (without attack – Type of Attack); column 3 (WS): the amount of white spaces slots; column 4 (TV): the amount of slots busy for the TV Towers. Table 2 is formed by 6 columns, namely: column 01 (Nr of attackers), amount of attackers simulated in one slot; column 02 indicates the type of transmission (without attack – Type of Attack); column 3 (CR's Tx): amount of CR's to transmit for simulation; column 4 (CR's i): amount of CR's that they had transmitted; column 5 (PC Tx): number of packages to be transmitted, e; finally, column 6 (PC Tx): number of packages effectively transmitted. In Table 1 and Table 2 the twirled referring data to first and the last ones of each above-named item have been represented. We can observe in Fig 3(b), 3(c) and 3(d), the degradation of the network related to the number of radios that had not the chance to transmit when the attacks were inserted in the simulations, when compared the transmissions without the insertion of attacks Fig 3(a). We notice that when the attacks are executed together, about 35 attackers, the network loses its capacity of opportunistic occupation of the spectrum.

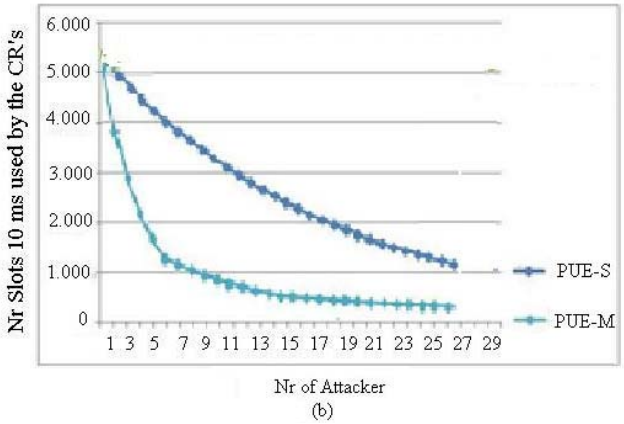
Table 1: Data of the Rounds of Simulation (for slots of time)

(1) Amt.	(2) Type of Attack	(3) White Space	(4) Tx TV
0	**Without**	1.734.167	1.865.033
1	**PUE S**	1.632.115	1.657.182
30	**PUE S**	1.687.557	1.626.369
1	**PUE M**	1.575.944	1.716.623
30	**PUE M**	1.605.428	1.774.777
1	**SSFF-AFr**	1.655.456	1.889.362
30	**SSFF-AFr**	1.784.063	1.678.762
1	**SSFF-AB**	1.551.707	1.815.660
30	**SSFF-AB**	1.764.731	1.619.580
1	**SSFF-AFa**	1.768.732	1.801.576
30	**SSFF-AFa**	1.717.718	1.885.747
5	**All**	1.660.131	1.670.717
150	**All**	1.648.468	1.845.401

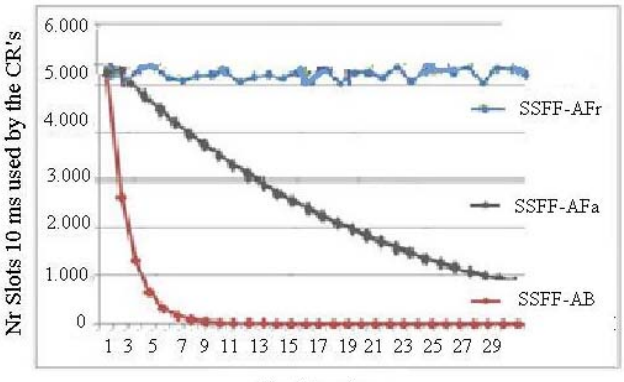
Table 2: Data of the Rounds of Simulation (for slots of time)



(a)



(b)



(c)

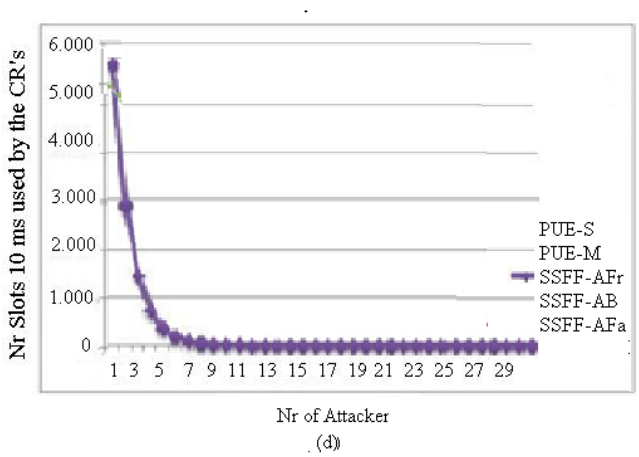


Figure 2. Simulation that presents the comparisons of the effect of the attacks: (a) Without attacks ; (b) Effect of Attacks PUE; (c) Effect of Attacks SSFF, and; (d) Effect of the Combination of All the Attacks..

When analyzing each type of attack, as well as the performance of the detection mechanisms isolated. The detection of the PUE-S attack has an average rate of TP of 42.05%. In the PUE-M attack is 34.54%. This difference can be justified in virtue of the greater aggressiveness the PUE-M attack that has the purpose of really affecting network transmission. In contrast of the attack of PUE-S has the as purpose to use of free channels selfishly. We observe the TP rates when the reputation mechanism is used isolated for SSFF attacks detection. The rates measured had been: 44.51, 42.64 and 33.22, for the SSFF-AFr, AFr and AB attacks respectively. The aggressiveness of the attack reflects in the detection

4.3 Adjusting the threshold of Acceptability and the Coefficient of Normalization

Table 3: TVA Representative of the Rounds of Simulation

TVA	12	13	14	**15**	16	17	18
TP	50	‘50	50	49,43	49,01	48,9	50
FP	0,16	0,99	1,67	2,69	3,11	3,97	2,97
FN	0	0	0	0,57	0,99	1,1	0
TN	49,84	49,01	48,33	47,31	46,89	46,03	47,03

In this experiment variations for the TVA of the CRs have been carried through, as well as the normalization value of the credibility normalization constant (VNC) of the radios with intention to adapt the analysis of the reputation mechanism with the localization mechanism. Initially the TVA and the VNC are 15 and 5.51 have been fixed, respectively [27]. In each simulation round, 1.440 evaluations of the mechanism had been carried through, the mechanism carries through this evaluation in regular intervals of 2.5 seconds, totalizing in the 30 rounds (combinations of the attacks): 43.300 evaluations. Table 3 presents the results achieved in this experiment for TVA; Table 4 presents the results achieved in this experiment for the VNC, and; Table 5 presents the results received with the variation of TVA and the VNC together; It is observed that: in the joint mechanisms simulation, as much with the increase, as with the reduction of the TVA to 13, and of the

Increase, as with the reduction of the TVA to 13, and of the VNC, to 5.49 occurs an increase in the values of FP and FN.

Table 4: Value of the Coefficient of Normalization (VNC) of the Rounds of Simulation

VNC	5.48	5.49	5.50	**5.51**	5.52	5.53	5.54
TP	50	50	50	49,43	49,01	48,9	50
FP	0,16	0,99	1,67	2,69	3,11	3,97	2,97
FN	0	0	0	0,57	0,99	1,1	0
TN	49,84	49,01	48,33	47,31	46,89	46,03	47,03

In the analysis of TVA and the VNC with values 14 for TVA and value 5.50 for the VNC, we get the best values of FP and FN. As our study case gives priority to the intrusion detection with the use in set of the two mechanisms, we work with the TVA = 14 and the VNC = 5.50.

After the calibrations have been carried through more 10 simulation rounds using the TVA=14 and the VNC=5.50. It had the insertion of all the attacks in its maximum configuration, that is, 30 attackers of each type. The results were: TP=45.14, TN=48.66, FN=4.86 and FP=1.34. These values, when compared [18] with one average rate of VP=44% and [27] VP=43.18%, demonstrate that the combination of the mechanisms in the intrusion detection PUE and SSFF has a better performance.

Table 5 TVA/VNC Representative of the Rounds of Simulation

TVA	12	13	14	**15**	16	17	18
VNC	5.48	5.49	5.50	**5.51**	5.52	5.53	5.54
TP	**5.48**	**5.49**	**5.50**	**5.51**	**5.52**	**5.53**	**5.54**
FP	45,85	46,45	**47,05**	46,42	45,59	45,56	44,98
FN	2,97	0,91	**0,16**	1,25	2,69	3,11	3,97
TN	4,15	3,55	**2,95**	3,58	4,41	4,44	5,02

4.4 Calibrating the Weights of the Mechanisms of Detention

After the previous stages, a great mass of data was produced. We divided this mass in two groups: One is used to train the genetic algorithm to associate weights to the detection mechanisms and another for the evaluation. We define then the DLR_i function (8) as:

$$D LR_i = \gamma L + \omega R; \quad (8)$$

$$DLRi = (\gamma_1 L_1 + \gamma_2 L_2) + (\omega_1 R_1 + \omega_2 R_2 + \omega_3 R_3). \quad (9)$$

As we are able to see the DLR_i function has 5 chromosomes function (9) - the Localization mechanism is represented by two chromosomes: L_1: PUE Selfish attack detection mechanism, and; L_2: PUE malicious attack detection mechanism. The Reputation mechanism is represented by three chromosomes: R_1: SSFF-AFr attack detection mechanism; R_2: SSFFAB attack detection mechanism and; R_3: SSFF-AFa attack detection mechanism. Each chromosome is composed of 30 genes, forming the first generation. Each set of genes (chromosome) forms a weight vector. Each gene, varying of [0-1], represents the weights of each mechanism (γ for the mechanisms of Localization, and ω for the mechanisms of Reputation). The crossings, elections and mutations for a total number of 100 generations in the 30 rounds of simulation with all are carried through the attacks. The representative values of the weights that consist of the solution that corresponds to the point of maximum of the DLR_i function is:

$$DLRi = (\mathbf{0,199}L_1 + \mathbf{0,321}L_2) + (\mathbf{0,03}R_1 + \mathbf{0,342}R_2 + \mathbf{0,103}R_3). \quad (9)$$

We can observe that the weights attributed for the GA agrees with the reality of the CRN degradation (Figure 2), where the most aggressive observed attack is SSFF-AB, whose weight of 0.342 is the biggest value in the detection function. In the same way the weight for the attack detection SSF-AFr, 0.035, reflects an attack of lesser expression, when compared to the others. Applying the mechanism with the weights for the GA to the training mass we get, Table 6:

Table 6. Mechanisms Calibrated simulated in set with all the agreed attacks

Atc	5	25	50	75	100	125	150	Avg
TP	50,00	50,00	50,00	49,31	44,87	38,45	34,29	45,65
FP	0,00	0,00	0,00	0,69	5,13	11,55	15,71	4,35
FN	0,00	0,00	0,00	0,00	1,16	3,02	5,15	1,23
TN	50,00	50,00	50,00	50,00	48,84	46,98	44,85	48,77

Finishing, table 7, a new mass of data, different of the data used for training GA, is analyzed with the detection mechanism, now weighed for the detection function, which resulted in a increased TP rate in about 0.5 percentile point, that is: TP=45.63, demonstrating that really it has the necessity of attribution of weights for the agreed detection of attack to the CRNs.

Table 7. Mechanisms Calibrated simulated in set with all the agreed attacks

Atc	5	25	50	75	100	125	150	Avg
TP	50,00	50,00	50,00	49,44	44,91	38,54	34,33	45,63
FP	0,00	0,00	0,00	0,56	5,09	11,46	15,67	4,37
FN	0,00	0,00	0,00	0,00	1,26	3,12	5,34	1,24
TN	50,00	50,00	50,00	50,00	48,84	46,98	44,85	48,76

4. Related Work

It was considered in [21], a method for PUE detection, based on the Euclidean calculation of the radio positioning, as well as the communications tower. The localization coordinates then are used for analysis and to label the degree of trustworthiness of each radio. The proposal is based on the previous knowledge of the positioning and the power of transmission of all CR, as well as of the PU. However the work defines its hypothesis of detection in a cooperative scene, where the primary radios transmit control information, between them: positioning, power of transmission, etc.; opposing the norms of the FCC [6], that no alteration in the infrastructure and the configurations of the primary networks should be made with the purpose to adapt it to the new CR technology. Our proposal is very different from the work above considered, therefore, beyond the analysis for the decision of detection of the attack to be also based on the behavior of the radios; our proposal does not have the necessity of any information supplied by the PU. SSFA attack was mentioned first in [14] and for [22 and 23]. In [22] the detection of the counterfeited data was carried through using a based mathematical approach in the sequential relation of probability, with good results. However this method demands the previous knowledge of the physical position of all the constituent elements of the network, including the position of the primary base station, being improper for use in mobile networks, beyond the necessity of the positioning of all the radios, information it is not always possible to have In [3], it was considered an algorithm for data fusion and for testing the counterfeited data detection, also for mobile networks, and without the necessity of previous knowledge of network elements localization. However, the considered detection approach is extremely vulnerable to noises and interferences, and also the detection stage does not make distinction between modulated signals, noises and interferences. The our proposal is different because our decision mechanism is based on CR transmission power detection, as well as, to not only make an added Mannering analysis to the analysis of the degree of reputation of each radio. We find in [12] the description and the framing of five categories of specific attacks to CRN. The proposal presents a generalization and an aiming to the forms of mitigation of

these types of attacks. Considering the PUE attack, it recommends the exchange of digital signature that allows each receiver to verify if the source is a legitimate user or not. Not being able to follow such recommendation because it opposes the specifications of the FCC to the installation of the cognitive apparatus without any alteration of the configurations of the primary network. The proposal described in [18] specifies a form of determination of PUE attack. The work considers the detection of the level of energy of the emitted signal, beyond the localization of the transmitters. The work is based on the following assumptions: (i) the primary transmitters are TV Towers with a known position fixed and with high power of transmission (in the scale of hundreds of kilowatts), and (ii) the CRs are devices with the limited power of the transmission (that it varies from *miliwatts* to some *watts)*. A localization algorithm, called *LocDef*, associates the calculation of energy emission of the main antenna for its detection. However, it has the necessity to use a secondary sensor network to execute such calculations, called Localization Verifiers, becoming these points' vulnerable elements to new attacks. In this presented proposal, the necessity of a secondary network for such calculations does not exist; therefore the analysis is carried through individually, for each radio, as well as of cooperative form for all network.

5. Conclusions and Future Work

In the present work we propose an Intrusion Detection System that is based on the composition of two detection mechanisms, namely the Localization Mechanism and the Reputation Mechanism. To validate our proposal, we applied our proposed IDS to scenarios with the presence of two kinds of Primary User Emulation attackers and three kinds of False Feedback attackers. The results show that the combined use of different detection mechanisms can be successfully applied in scenarios with the presence of several kinds of attackers. We additionally determined an optimized calibration of the weights of the mechanisms with the aid of Genetic Algorithms. The results show a sensitive improvement of the "calibrated" IDS compared to the "nocalibrated" one. While the investigated scenarios were composed of several types of attackers, each attacker had a "pure" behavior, in the sense that a PUE-S attacker only performed PUE-S attacks. In future works, we intend to analyze the performance of our proposed IDS in the presence of "smarter" attackers that change their attacks behavior during simulation. We believe that this kind of scenario is the one where the combination of detection mechanisms can be more advantageous.

References

[1] Akyildiz, Ian (2006), F.; Vuran, Mehmet C.; Lee, Won-Yeol; Mohanty, Shantidev. "Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks:A Survey". Computer Networks, N. 50.

[2] Akyildiz, Ian, (2008). F., Lee, Won-Yeol, Vuran, M. C., & Mohanty S., "A Survey On Spectrum Management In Cognitive Radio Networks". Ieee Communications Magazine, Vol. 46, Issue 4, Pp. 40-48

[3] Cabric, D. (2004), Mishra, S.M., Brodersen, R.W.: "Implementation Issues in Spectrum Sensing for Cognitive radios". In: Conf. Record of the 38th Asilomar Conf. on Signals, Systems and Computers, vol. 1, pp. 772–776

[4] Clancy T, (2008) Goergen N. "Security In Cognitive Radio Networks: Threats And Mitigation". Third International Conference On Cognitive Radio Oriented Wireless Networks And Communications (Crowncom),;

[5] Clancy T, (2009), A. Khawar, "Security Threats to Signal Classifiers Using Self-Organizing Maps", Fourth International Conference On Cognitive Radio Oriented Wireless Networks And Communications (Crowncom)

[6] FCC, Federal Communication Commission (2009) Home Page. Http://Www.Fcc.Gov Last Acess in 13/10/2009.

[7] Ganesan G. (2005) And Y. Li, "Cooperative Spectrum Sensing In Cognitive Radio Networks," *Proc. Dyspan*, Nov.

[8] Hata(1980), M. Empirical formula for propagation loss in land mobile radio services, IEEE Transactions on Vehicular Technology, vol. 29, no. 3, pp. 317-325, Ago

[9] He T., (2003) C. Huang, B. M. Blum, J. A. Stankovic, And T. F. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," Proc.Acm Mobicom, Sept.,

[10] K. Jain (2003), J. Padhye, V. N. Padmanabha, and L. Qiu, "Impact of interference on multi-hop wireless network performance," Proc. ACM Mobicom, Sept. 2003, pp. 66–80.

[11] Lacerda, (1999) E.G.M e Carvalho, A.C.P.L. "Introdução aos algoritmos genéticos", In: Sistemas inteligentes: aplicações a recursos hídricos e ciências ambientais. Editado por Galvão, C.O., Valença, Porto Alegre.

[12] Leon, Olga (2010), Juan Hernandez-Serrano, Miguel Soriano. "Securing Cognitive Radio Networks".International Journal Of Communication Systems, Vol 23,. Issn/Isbn

[13] Matew V. (2002) Genetic Algorithm Department of Civil Engineering, Indian Inst of Technology Bombay, Mumbai-400076.

[14] Mishra, S.M (2006)., Sahai, A., Brodersen, R.W.: Cooperative Sensing Among Cognitive Radios. In: Ieee International Conf On Com, Icc 2006, 1658–1663

[15] Mitola, J (2000). "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio". Ph.D. Dissertation, Kth RIT, Stockholm, Sweden.

[16] M. Mchenry (2003)., "Frequency Agile Spectrum Access Technologies," in *FCC Workshop on Cognitive Radio*, May

[17] Nhan Nguyen-Thanh (2009), Insoo Koo, "A Secure Distributed Spectrum Sensing Scheme in Cognitive Radio", Proceedings Of The Intelligent Computing 5th International Conference On Emerging ICTA, Sep 16-19,, Ulsan, S Korea

[18] Park J (2008).-M. R. Chen, , And J. H. Reed, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE Journal On Selected Areas In Communcations Special Issue On Cognitive Radio Theory And Applications, Vol. 26,

[19] Roos T. (2002), P. Myllymaki, And H. Tirri, "A Statistical Modeling Approach to Location Estimation," Ieee Trans. Mobile Computing, Vol. 1, Jan.-March, P 59–69.

[20] Shankar U., N Sastry, U. and D. Wagner, "Secure verification of location claims," in Proceedings of the ACM workshop on Wireless security (WiSe), San Diego, 2003.

[21] Sherestha J.; (2010). Sunkara, A.; Thirunavukkarasu, B. Security in Cognitive Radio. San Jose: State University.

[22] Ruiliang C. (2008a), Jung-Min, P., Hou, Y.T., Reed, J.H.: Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks. IEEE Communications Magazine

[23] Ruiliang, C (2008B)., Jung-Min, P., Kaigui, B.: Robust Distributed Spectrum Sensing inCognitive Radio Networks. In: IEEE The 27th Conference on Computer Communications, INFOCOM 2008, pp. 1876–1884

[24] Silva, G. (2009), "Intrusion Detection in computer networks: Immune-inspired algorithm based in the Danger Theory and the Dendritic Cells", Master Thesis, UFMG, March 2009.

[25] T. Fawcet (2005). An introduction to roc analysis. *Pattern Recognition Letters*, 27:861{874, 2005.

[26] Wild B., K. (2005) Ramchandran, "Detecting primary receivers for cognitive radio applications," Proc. DySPAN,

[27] Zhu,Feng (2009) and Seung-Woo Seo, "'Enhanced Robust Cooperative Spectrum Sensing in Cognitive Radio", JCN, Special Issue on Cognitive Radio: A Path in the Evolution of Public Wireless Networks, Volume 11, Pages 122-132,

Joffre Gavinho Filho a M.Sc. Student at the Federal University of Rio de Janeiro (UFRJ), Brazil. His research interests include Cognitive Radio, Wireless Networks and Network Security.

Luiz Fernando Rust da Costa Carmo received a Ph.D. degree on Computer Science in 1994, French, (LAAS/CNRS). His research interests include formal description techniques, communication networks, embedded systems and information security.

Raphael Machado received a Ph. D. degree on Engineering of Systems and Computation in the COPPE/UFRJ (2010). His research interests include Theory of the Computation, Telecommunications Protection of Software and Smart Grids.

Luci Pirmez She received her Ph.D degree in computer science from the UFRJl in 1996. Her research interests include wireless networks, wireless sensor networks, network management and security.