O. Leon, R. Roman, and J. Hernandez Serrano, "Towards a Cooperative Intrusion Detection System for Cognitive Radio Networks", *Workshop on Wireless Cooperative Network Security (WCNS11)*, LNCS, 2011.
http://doi.org/10.1007/978-3-642-23041-7_22
NICS Lab. Publications: https://www.nics.uma.es/publications

Towards a Cooperative Intrusion Detection System for Cognitive Radio Networks

Olga León[1], Rodrigo Román[2], and Juan Hernández-Serrano[1]

[1] Universitat Politècnica de Catalunya
{olga,jserrano}@entel.upc.edu
[2] Universidad de Málaga
roman@lcc.uma.es

Abstract. Cognitive Radio Networks (CRNs) arise as a promising solution to the scarcity of spectrum. By means of cooperation and smart decisions influenced by previous knowledge, CRNs are able to detect and profit from the best spectrum opportunities without interfering primary licensed users. However, besides the well-known attacks to wireless networks, new attacks threat this type of networks. In this paper we analyze these threats and propose a set of intrusion detection modules targeted to detect them. Provided method will allow a CRN to identify attack sources and types of attacks, and to properly react against them.

Key words: CRNs, IDS, security, PUE

1 Introduction

Traditionally, spectrum allocation has followed a static policy so that specific bands have been assigned to particular services operating under license. This fact and the huge increase in new wireless applications during the last years has led to the lack of spectrum for emerging services. In addition, according to the Federal Communications Commission (FCC) most of the spectrum is vastly underutilized [1]. Cognitive Radio Networks (CRNs) [2, 3] are regarded to be a possible solution to this problem by making use of the spectrum left unoccupied by licensed services or primary users. Thus, as secondary users of the spectrum, CRNs must be capable of identifying white spaces or vacant bands and select the best portion in order to operate while avoiding interferences to primary users. This implies that, whenever the presence of a primary is detected in the CRN operation channel, it must switch to another band, a process known as spectrum handoff.

The term *cognitive radio network* was first defined by Mitola [4] as a "network of cognitive radios". Cognitive Radios (CRs) are smart radios that sense the Radio Frequency (RF) environment (a process named spectrum sensing), make intelligent decisions based on sensing measurements and stored past data (i.e. selecting the channel with best conditions), and reconfigure themselves accordingly.

According to whether decisions are taken locally or by means of a base station which collects information from all nodes, CRNs can be classified into distributed or centralized networks. In its turn, in distributed CRNs decisions can be taken in an isolate manner by a CR on its own, or in a cooperative way by taking into account the reports provided by a set or all members of the CRN. On the other hand, sensing information can be exchanged by means of the data channel (in-band) or by using a dedicated control channel (out-of-band). Furthermore, several CRNs may overlap sharing the spectrum left by primary users (known as self-coexistence) and, consequently, there is also a need for mechanisms to enable coexistence among existing CRNs.

There are a few proposals on CRNs [5] following the different topologies above mentioned, but most research has focused on the on-going standard IEEE 802.22 [3] for Wireless Regional Area Networks (WRANs). This standard defines a centralized CRN operating in a point-to-multipoint basis, formed by a a base station and a set of nodes attached to the base station via a wireless link. IEEE 802.22 WRANs are designed to operate in the TV broadcast bands while assuring that no harmful interference is caused to primary transmissions, i.e., digital TV and analog TV broadcasting, and low power licensed devices such as wireless microphones. The set of CRs perform sensing during quiet periods scheduled by the base station, in which any transmission is allowed within the CRN in order to minimize any interference from the WRAN system to the sensing receiver. Then, sensing information is reported in-band by the CRs to the station, which is responsible for taking the final decision about the existence of a primary user.

Although research on CRNs has already been object of a big effort, it is still a hot topic requiring further work and, particularly, with regard to network security. As for any other network scenario security is usually split into two lines of defense. The first one is focused on avoiding attacks and it is closely related to the use of cryptographic primitives. The second one should be more devoted to detect and identify the attacks that have passed over the first line. IDSs behave as a second line of defense, where these mechanisms can identify the existence of an intrusion and the (possible) source of the attack, and notifying the network and/or the administrator so that appropriate preventive actions can take place [6].

This paper provides an overview of the new vulnerabilities and attacks to CRNs and proposes guidelines to design mechanisms to efficiently detect and counteract them. Those mechanisms are described in the context of an Intrusion Detection System (IDS), since these new threats cannot be yet overcome by the first line of defense.

The structure of the paper is as follows: Sect. 2 describes the main threats to CRNs appeared in the literature. In Sect. 3 we identify the requirements and main concepts regarding to the implementation of an IDS for detecting such attacks. Next, in Sect. 4 we provide a high-level description of its structure and the tasks to be performed by each of its components. Finally, in Sect. 5 we present the conclusions and future lines of the work.

2 New Threats in CRN

Falling into the category of wireless networks, CRNs inherit most of the threats already studied by the research community, such as Jamming attacks, selfish behaviors, eavesdropping, etc. However, due to the particular attributes of CRNs its impact on network performance may be different and also new security implications arise. Although this topic has received far less attention than other areas of cognitive radio, most of the work has focused (in decreasing order of importance) on four specific attacks: the Primary User Emulation (PUE) attack, specific attacks to cooperative sensing mechanisms, the Objective Function (OF) attack and the Lion attack targeted to disrupt TCP performance.

2.1 PUE

In a PUE attack, first coined in [7], an attacker pretends to be a primary user or incumbent by transmitting a signal with similar characteristics to a primary signal or replying a real one, thus preventing the CRN form using a vacant band. The impact of this attack depends on several factors, such as the location of the attacker and the sensibility of CRs in their measurements. Selecting an optimal position to perform the attack will cause many secondary users concluding that a given band is occupied and looking for another portion of the spectrum. On the other hand, if an energy-based method [8] is used to detect primary users, the threshold value will also play an important role: the lower the threshold is the easier to perform a PUE attack. As a consequence, there is a need for providing effective methods in order to distinguish between a legitimate primary transmission and a fake one (PUE attack). Moreover, based on previous knowledge of the CRN operation, an attacker can force PUE attacks whenever the CRN switches from one channel to another (frequency handoff) thus degrading the data throughput of the CRN or completely producing a Denial-of-Service (DoS) attack. To get this behavior, the attacker should estimate the next CRN operation channel in a limited time by:

- Sensing the media till find the new channel of operation. The attacker could discard some channels (e.g. channels already in use by primary transmissions) in order to minimize the channel search time. Moreover, the attacker can estimate the more probable new CRN channel based on its own local sensing.
- Eavesdropping the common control data of the CRN (if exists). IEEE 802.22 WG is aware of this threat and recommends securing all control data.

Detecting PUE attacks poses two new main challenges for the detection mechanisms: 1) applying location algorithms to precisely pinpoint the position of the emitter; and 2) developing an anomaly or signature based scheme that, once the emitter is located helps the detection mechanism to detect abnormal emitter's behavior. The former can overcome any PUE attack based on impersonating a TV emitter, since position of legitimate TV towers is assumed to be known, and can at least localize a wireless microphone emitter. The latter would also allow the CRN to, once the wireless microphone emitter is located, identify the PUE attack by analyzing anomalous behavior patterns.

There are a few state-of-the-art proposals dealing with PUE attacks mainly based on the analysis of the received signal power [9, 10]. However, these proposals assume that the attacker has a limited transmission power and/or the attacker is always located within the CRN. In [11], an approach similar to random frequency hopping is presented where secondary users randomly select a channel to transmit among those available.

2.2 Attacks to Cooperative Sensing

Cooperative sensing in CRNs [12, 13] allows taking a decision about the presence of a primary user in a given channel, based on the reports provided by a set of CRs. Each secondary user senses the spectrum individually and shares its results with the rest of the nodes in order to improve detection probability. As a consequence, malicious and selfish behaviors can arise, such as a malicious node which deliberately report false measurements leading to false positives or negatives or a selfish node, which do not cooperate in order to save energy, for instance. Often these attacks are aimed at improving the chances of a successful PUE attack.

2.3 OF Attacks

Objective Function (OF) attacks [14] are targeted to disrupt the learning algorithm of CR devices. Within a CRN, incumbents control several radio parameters in order to enhance the network performance. The parameters choice is often done by means of an artificial intelligence algorithm that makes slight modifications of several input factors to find their optimal values that maximize an objective or goal function. An attacker can alter the performance of the learning algorithm to its own profit by intentionally degrading (e.g. by jamming) the channel when some input factors are greater than a certain threshold. As a naïve example, the attacker can jam the channel whenever the security of the protocol is set and hence the learning algorithm will conclude that it is better to work without any security.

Since the OF attack was presented [14] in 2008, the scientific community hasn't paid too much attention to it since it does not apply to WRAN 802.22 [3], which is the most typical CRN scenario and the only standard regarding such networks. The fact is that WRAN defines a centralized scenario where all the "cognitive" behavior falls under the base station responsibility. However, the threat will affect a CRN actually made of cognitive radios and thus a complete IDS for CRN should take it into account.

2.4 Lion Attack

Finally, the Lion attack [15, 16] is a cross-layer attack targeted to disrupt TCP connections by performing a PUE attack in order to force the CRN network to switch from one band to another (frequency handoff). The interruption of

communications at specific instants can considerably degrade TCP throughput, or, if the attacker can predict or know the new transmissions parameters to be used by the sender after the handoff, actually turn into a permanent Denial of Service (DoS).

3 Implementing an IDS for CRNs

3.1 Background on IDS

As shown by the previous section, there are multiple types of attacks that can affect the performance and integrity of CRNs. The development of a first line of defense, such as cryptographic primitives to protect the exchange of common control data, is actually compatible with the deployment of a second line of defense that detects an attack on the precise moment it is targeting the network. This is the role of Intrusion Detection Systems (IDSs). Although widely used in wireless networks, IDSs have their own issues that must be considered, such as the existence of attacks against the medium itself, the distribution of the detection entities, and the need of a lightweight detection structure. These issues have been studied by the state of the art on this area [17], and will be explained in the next paragraph.

Regarding the distribution of the detection entities, a CR can take the role of monitoring the data it manages and its surroundings. If the evidence is inconclusive or there is a need to have a holistic point of view of the situation, the CR can make use of the distributed nature of the network and use a collaborative mechanism (with mechanisms to manage uncooperative CRs) to take a global intrusion detection action. Note that even in centralized CRNs (such as WRANs), the existence of distributed detection entities can help to develop a more accurate IDS. As for the attacks against the medium, not only the IDS can include specific components to detect these attacks, but it can also provide some cross-layer functionality where information from different network layers are used as an input to the components. Finally, it has been shown that even in extremely constrained distributed networks, such as wireless sensor networks (WSN), it is possible to design and deploy a functional IDS [18]. CRNs are not as constrained as these networks, thus they can be able to afford the existence of an IDS detection entity in every CR. Nevertheless, the behavior of the detection mechanisms should be highly optimized, as mentioned in [19].

After these issues have been discussed, it is necessary to describe the potential architecture of an IDS entity for distributed systems (i.e. the IDS entity located in a CR). In fact, there is a "de-facto" agreement on its basic elements [20]: a local packet monitoring module that receives the packets from the neighborhood, a statistics module that stores the information derived from the packets and information regarding the neighborhood, a local detection module that detects the existence of the different attacks, an alert database that stores information about possible attacks, a cooperative detection module that collaborate with other detection entities located within the neighborhood, and a local response module that take decisions according to the output of the detection modules.

Focusing on the detection modules used in these IDS for CRNs, they must make use of first-hand information, second-hand information, statistical data, and the data acquired by the CRs during its normal operation. These modules can then use this data to distinguish between normal and abnormal activities, thus discovering the existence of intrusions. There are actually three main techniques that an IDS can use to classify actions: misuse detection, anomaly detection, and specification-based detection [21]. The first technique compares the collected information with predefined "signatures" of well-known attacks. The second technique store patterns of what can be considered as "normal" behaviour, and react against any significant deviation of those patterns. Finally, the third technique is also based on deviations from normal behavior, although the concept of normal behavior is based on manually defined specifications instead of on machine learning techniques and training. All these three techniques can be used in the context of a CRN, such as a signature-based scheme to detect Lion Attacks, or an anomaly-based technique to detect OF attacks.

3.2 IDS Requirements and Attacker Model

When designing the blueprint of the IDS and the functionality of its detection modules, presented in Sect. 4, it is necessary to consider both certain requirements that the elements of the IDS must fulfill and the attacker model that specifies the capabilities of the adversaries that target the services of the CRNs. Regarding the IDS requirements, these are the most relevant [17]:

- The IDS must not introduce new weaknesses into the system. For example, the cooperative detection module must take into account the existence of malicious and faulty nodes, and the existence of DoS attacks targeting the IDS message management systems must be prevented.
- The IDS must be fault-tolerant, able to run continuously and recover from problematic situations. The existence of mechanisms that store the current and previous state of the IDS must be considered in the design.
- The IDS must provide adequate mechanisms that allow users or the network itself to know about the existence of a certain attack an react against it. This includes attacks against the IDS itself.
- The design of the IDS must allow the addition of new detection modules, or a seamless interaction with existing detection mechanisms. Note that any detection module must be as accurate as possible, with fewer false positives and false negatives.

As for the attacker model, the model described in this paragraph focuses on the capabilities of the attackers. For example, we assume that the *knowledge* of the attacker can be quite diverse. He can know nothing about the structure of the CRN, trying to learn about it by eavesdropping or implementing some known fuzzy logic techniques [14]. Or he can have complete knowledge about the CRN operation, which enables him to perform sophisticated attacks such as OF or the Lion attack. Regarding his *transmission power*, we will assume that most attackers will make use of small radios with a limited action range, but we will not discard the existence of powerful emitters with the capacity of

faithfully emulating a primary TV signal. As for the *number of devices* owned by the attacker, it could range from one till many cooperating radio devices, which could difficult the operation of the IDS detection mechanisms. Finally, as the *mobility* of the attacker can degrade the functionality of the IDS, we will assume that the attacker can both move within a given area and remain static at a fixed position.

4 A Blueprint for an IDS Suited to CRNs

In this section we will define the blueprint of an IDS for CRN, which will contain the different detection mechanisms for the attacks described in Sect. 2. Such blueprint can be used as a foundation for the creation of a functional and usable IDS. The architecture of the IDS is shown in Fig. 1, and includes the following modules: input, memory, output, and detection. The *input module* is in charge of managing the first-hand information, the second-hand information, and the cooperative processes. The *memory module* is used to store the statistical information derived from the input and to provide an interface to the specific network information managed by the CR. The *output module* takes decisions according to the output of the detection modules (e.g. it informs the user or a central system) and stores other information such as the alert database. Finally, the *detection module* detects the existence of the different attacks, using as an input the data provided by the input and memory modules. From now on we will focus on the modules or sub-modules composing the detection module. Fig. 1 sketches the different modules with their relationships. Note that this IDS blueprint is not exclusive, as it can be possible to add new detection mechanisms that will take advantage on the existence of the input, memory, and output modules.

4.1 Module of Cooperative Location of Primary Emitters

As afore-mentioned, locating a source of real or fake primary transmissions may lead to mitigate or at least effectively react against PUE attacks. Physical location of RF transmission sources has been a hot topic for many years in wireless applications, but most of the proposals in the literature rely on measures of certain distance dependent parameters performed at the BS or at nodes whose position is well known. Typically, these parameters are [22]: 1) received signal strength (RSS), based on the fact that signal strength varies inversely with the square of the distance in free space; 2) the time taken by the signal to travel between two nodes, which allows to estimate the angle of arrival (AOA) or the time of arrival (TOA) but which requires cooperation of the locating node; and 3) the difference time of arrival (TDOA), which utilizes cross-correlation processes to calculate the difference in time of arrival of the emitter signal at two or higher pairs of nodes.

From the above commented techniques, we consider TDOA to best suit the IDS requirements since RSS is susceptible of high errors due to the dynamics of outdoor environments (multipath signals and shadowing) and TOA/AOA

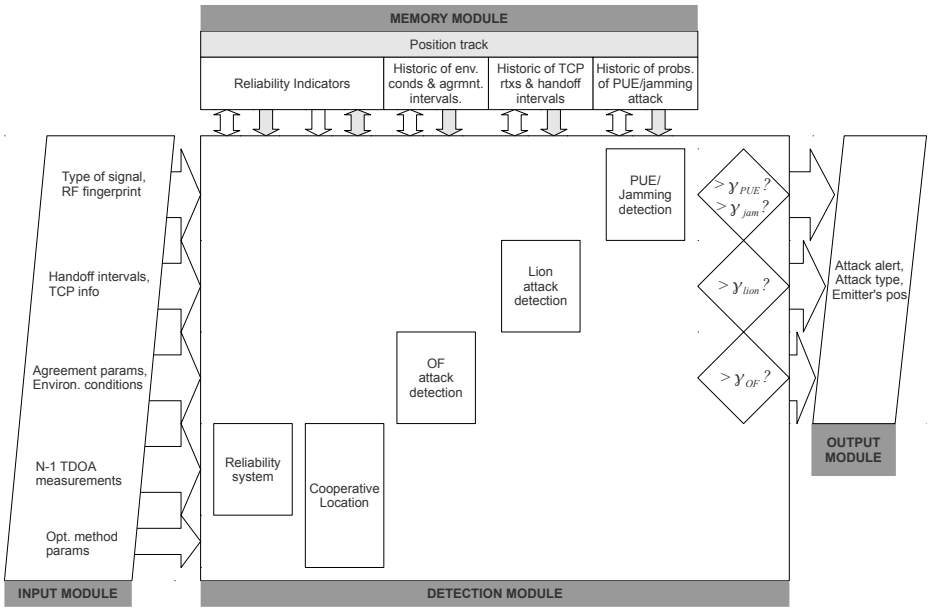

Fig. 1. Modules of a cooperative IDS for CRN

requires cooperation of the node to be located and, since we aim to determine the position of potential attackers, any cooperation from the node we wish to locate cannot be expected.

TDOA techniques require at least two TDOA measures (cooperation of 3 nodes) to locate an emitter on a surface and three measures (at least four nodes) to locate the emitter on the 3-dimensional space. These measures lead to a linear system of equations that can be easily solved [23]. However, in practice measurements are subjected to errors and then a solution of the system can be rarely found. In this case, the location problem can be posed as an optimization problem and solved using, for example, a least squares (LS) estimations such as Taylor [24] or extended Kalman-Bucy filter [25], which can be a better choice for mobile sources. Consequently, the accuracy of the estimation will depend on the number of TDOA measurements and thus on the number of cooperating nodes.

We represent the cooperative location module as a box, see Fig. 1, with the following inputs and outputs:

From input module:

- $N-1$ TDOA measurements obtained as the differences between the primary signal measure obtained by the node implementing the module and the same measure at other $N-1$ cooperating nodes.
- Necessary parameters for the chosen optimization method. As stated before, the optimization can be based, for example, on least squares (LS) methods or on extended Kalman-Bucy filters and both require at

least an initial estimation of the position of the emitter, a covariance matrix and, in the latter case, a mobility pattern.

From memory module:

- An indicator of the reliability of the measurements based on previous results and computed by the reliability system module (section 4.2).
- Read access to the previously stored emitter's position and its associated estimation error, especially when estimating the position of mobile emitters.

To memory module:

- The estimated position of the primary emitter. The estimation position should follow the format $f(t) = (x, y, z)$ being $f(t)$ constant in time if the primary source is static and a mobility prediction otherwise.
- A guess of the error performed in the estimation of the position.

4.2 Module of Reliability System

This module is in charge of measuring the reliability of the TDOA measurements provided by a given CRN node. It computes the TDOA measurement that a given node should have taken according to the emitter's position estimated by the cooperative location module. This value is then compared with the TDOA measurement provided by such node. The greater the divergence is, the less reliability is assigned to that node's measurements. Obviously, the module should take into account past measurements of the same node.

From input module:

- $N - 1$ TDOA measurements obtained as the differences between the primary signal measure obtained by the node implementing the module and the same measure at other $N - 1$ cooperating nodes.

From memory module:

- The previously computed reliability indicators.
- The estimated position of the primary emitter made by the cooperative location method and its associated interval of error.

To memory module:

- Updated reliability indicators for any of the cooperating nodes reporting TDOA measurements.

4.3 Module for Detecting Jamming and PUE Attacks

Jamming attacks interfere with the CRN operation channel forcing the network to switch to another channel with better conditions. If the attack is repeated whenever the CRN switches, the throughput can be degraded or even starved at all. PUE attacks have the same purpose of jamming ones but differ in that they emulate primary transmissions instead of just producing noise. In 802.22, PUE attacks can be classified depending on the type of the primary signal into TV signal-based and wireless microphone-based attacks.

Attacks based on jamming or wireless microphone-based PUE may be detected with an anomaly detection IDS module: jamming/PUE appearing whenever the CRN switches from one channel to another. As a result this module should be able to identify and attacker "following" the CRN. This can be achieved by estimation of the attacker's current and future position (with a given mobility pattern) and/or its Radio Frequency Fingerprint (RFF).

TV signal-based PUE attacks can be more easily overcome since legitimate TV primary emitters' positions are assumed to be fixed and known. As a result just comparing the estimated position given by the cooperative location module with the database of TV emitters will clearly identify whether it is a PUE attack or not. In order to reduce the rate of false positives/negatives, RFF techniques [26] can be used to probabilistically recognize a predefined source of transmissions.

From input module:

- Type of signal: pure jamming, primary signal (e.g. TV or wireless microphone signals). Jamming would be any signal that is not a primary emission, e.g. TV or wireless microphone transmissions. Mechanisms for detecting primary signals have been widely studied and many proposals have appeared in the literature [27, 28].
- RFF of the primary emitter.

From memory module:

- The estimated position of the primary emitter made by the cooperative location method and its associated error.
- Previously computed probability of jamming/PUE attack for the current emitter (stored by it current position estimation or its RFF)

To memory module:

- Updated probability of jamming/PUE attack for the current emitter.

To output module:

- If the probability of being under a jamming attack is above a certain threshold γ_{jam}, the module outputs an alert of jamming attack by the current emitter.
- If the probability of being under a PUE attack exceeds a certain threshold γ_{PUE}, the module outputs an alert of PUE attack by the current emitter.
- If any of the previous is true, the module outputs the estimated position of the emitter and its associated error.

4.4 Module for Detecting Lion Attacks

This module relies on a signature-based scheme which looks for matches between instants of retransmission attempts for a given TCP connection and the beginning of a frequency handoff caused by the detection of a potential primary user. Whenever there is a match, the probability of being under a Lion attack is increased. Therefore, this module should take as input cross cross layer data (TCP retransmission instants and physical handoffs) provided by the input module, as well as past probabilities of being under attack provided by the memory module.

For example, let us consider a TCP connection with an initial retransmission timer of τ seconds. If a segment is lost due to a frequency handoff forced by an attack (jamming or PUE), it will be retransmitted after τ seconds. Since TCP's backoff algorithm doubles the retransmission timer with each unsuccessful attempt, next retransmissions will occur after $t = \tau, 3\tau, 7\tau, 15\tau, \ldots, (2^i - 1)\tau$ For common values $\tau = 200$ms and handoff intervals of 1.5s, retransmission instants are $200, 600, 1400, 3000, 6200, \ldots$ms. The first three retransmission attempts will obviously fail because they match the first handoff period, so we do not take them into account to compute the probability of attack. However, at $t = 1.5s$, the handoff has ended and the CRN is operating in a new channel, so new retransmissions should now succeed. If a malicious user is performing a Lion attack, it may predict the time of the next retransmission and force a new handoff, leading again to the failure of the next retransmission attempt. The attacker may repeat this process each time the CRN performs a frequency handoff, completely starving the TCP source. In a naïve implementation, if we define a module threshold of 4 retransmission failures out of the first handoff in order to have a probability of 100% of being under a Lion attack, with the fourth retransmission failure at $t = 3$s (first one after the first handoff) the module output will be a probability of $\frac{100\%}{4} = 25\%$, with the fifth ($t = 6.2$s) of 50%, etc. And so on until, with the sixth retransmission (the fourth out of the first handoff), we get a probability of 100% and an alert for this attack is reported.

From input module:

- The physical/MAC layer reports when the CRN is performing a handoff.
- The transport layer provides with the current TCP retransmission instants.

From memory module:

- Past TCP retransmission instants/attempts and physical handoff intervals.

To memory module:

- Current probability of being under a Lion attack for a given threshold for a given emitter.
- The module stores a log of TCP retransmission instants/attempts and physical handoff intervals.

To output module:

- If the probability of being under a Lion reaches 100% for a given threshold, the module outputs an alert of Lion attack by the current emitter, the estimated position of the emitter and its associated error.

4.5 Module for Detecting OF Attacks

The basis of this module is to detect abnormal environment conditions related to the use of some transmission parameters as security, modulation, codification, etc. Consequently it should store some statistics about the environment characteristics related to configuration profiles and check whether with some profiles it can be found a long deviation from the expected values. Correlation between agreement time intervals and abnormally bad environment conditions give us

a probability of being under an OF attack. If this probability becomes greater than a certain threshold γ_{OF} then an alert is generated.

From input module:

- Boolean indicating if there is an on-going parameter agreement and, being the case, the parameters in negotiation.
- Current environment conditions.

From memory module:

- Historic of environment conditions (normal values, variance, predictions, etc) and agreement time intervals.

To memory module:

- New environment data and agreement time interval.

To output module:

- If the probability of being under a OF attack is above a certain threshold γ_{OF}, the module outputs an alert of OF attack by the current emitter, the parameters under attack and the current estimated emitter's position.

5 Conclusions and Future Work

CRNs can improve the current inefficiency in spectrum usage by detecting which frequency bands are not being in use by licensed services. With this purpose, the set of CRs composing a CRN perform spectrum sensing and select in a collaborative way the best channel to operate, assuring that no harmful interference is caused to primary or licensed transmissions and the coexistence with other CRNs.

The specific mechanisms used in CRNs, such as spectrum sensing or cooperation among CRs, pose new security challenges that need to be properly addressed. In this paper we have presented an overview of the main new threats to CRNs appeared in the literature: the PUE attack, attacks to cooperative sensing, OF attacks and the Lion attack.

Traditional protection against attacks relies on a first line of defense based on proactive measures, such as confidentiality and authentication, and a second line that actually detects each attack and consequently get the chances to react against it. CRNs inherit the first line of defense from the wireless networks approach, however the design of a second line of defense suited to CRNs, such as an IDS, is still challenging.

The target of this paper has been to provide future researchers with the guidelines to implement a valuable IDS for the new threats to CRNs. Its design is intended to provide a container where these and other mechanisms can be implemented inside a device and interact with existing interfaces (e.g. the information stored inside the CR, the output of the different network layers). The proposed high-level scheme fulfills the standard requirements for an in-network IDS [17] and inherits the cognitive behavior of CRNs, which implies learning from the past, making intelligent decisions and positively evolving. We have focused on defining the necessary inputs (input module), the storage requirements

(memory module) and the attack alerts (output module) generated based on cognitive decisions (detection module) from present and past data.

Note that the elements described in this article are the first steps towards fully secure and fault-tolerant CRNs, thus more research is required to provide optimal detection mechanisms that will guarantee a safe change of paradigm. With security being a global issue spanning through all protocol layers and across all network elements, a chain is as strong as its weakest link. Therefore, no matter the efforts, if one layer is vulnerable, the whole network is. A promising future line of research is to propose standardized cross-layer interfaces for CRNs which allow to get the security to all its extent. An example of IDS module that would take profit of this research is our proposed Lion attack detection module, which implies communication between physical and transport layer.

Acknowledgements This work has been partially supported by the Spanish *Comisión Interministerial de Ciencia y Tecnología* (CICYT) with the project P2PSEC (TEC2008-06663-C03-01); the Spanish *Ministerio de Ciencia e Innovación* with the CONSOLIDER project ARES (CSD2007-00004) and the FEDER co-funded project SPRINT (TIN2009-09237); and the *Generalitat de Catalunya* with the grant 2007 GRC 01015 to consolidated research groups awarded to the Information Security Group of the *Universitat Politècnica de Catalunya* (UPC).

References

1. Federal Communications Commission (FCC): ET docket no. 03-322. notice of proposed rule making and order. (December 2003)
2. Akyildiz, I.F., Lee, W.Y., Vuran, M.C., Mohanty, S.: Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Comput. Netw. **50**(13) (2006) 2127–2159
3. Cordeiro, C., Challapali, K., Birru, D., Shankar, Sai, N.: Ieee 802.22: an introduction to the first wireless standard based on cognitive radios. Journal of Communications **1**(1) (April 2006) 38–47
4. Mitola, J., I.: Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis, Royal Institute of Technology (KTH), Sweeden (2000)
5. León, O., Hernández-Serrano, J., Soriano, M.: Securing cognitive radio networks. International Journal of Communication Systems **23**(5) (February 2010) 633–652
6. Bace, R.G.: Intrusion Detection. Sams (2000)
7. Chen, R., Park, J.M.: Ensuring trustworthy spectrum sensing in cognitive radio networks. In: 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR). (September 2006) 110–119
8. Cabric, D., Mishra, S., Brodersen, R.: Implementation issues in spectrum sensing for cognitive radios. In: Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers. Volume 1. (November 2004) 772–776
9. Chen, Z., Cooklev, T., Chen, C., Pomalaza-Raez, C.: Modeling primary user emulation attacks and defenses in cognitive radio networks. In: Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International. (December 2009) 208 –215

10. Jin, Z., Anand, S., Subbalakshmi, K.P.: Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. SIGMOBILE Mob. Comput. Commun. Rev. **13** (September 2009) 74–85
11. Li, H., Han, Z.: Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics. Wireless Communications, IEEE Transactions on **9**(11) (November 2010) 3566 –3577
12. Song, C., Zhang, Q.: Achieving cooperative spectrum sensing in wireless cognitive radio networks. SIGMOBILE Mob. Comput. Commun. Rev. **13**(2) (2009) 14–25
13. Mishra, S., Sahai, A., Brodersen, R.: Cooperative sensing among cognitive radios. In: Proceedings of IEEE International Conference on Communications, ICC'06. Volume 4. (June 2006) 1658 –1663
14. Clancy, T., Goergen, N.: Security in cognitive radio networks: Threats and mitigation. In: 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom). (May 2008) 1–8
15. León, O., Hernández-Serrano, J., Soriano, M.: A new cross-layer attack to tcp in cognitive radio networks. In: Second International Workshop on Cross Layer Design (IWCLD). (2009) 1–5
16. Hernández-Serrano, J., León, O., Soriano, M.: Modeling the Lion Attack in Cognitive Radio Networks. EURASIP Journal on Wireless Communications and Networking **2011** (2010)
17. Mishra, A., Nadkarni, K., Patcha, A.: Intrusion detection in wireless ad hoc networks. Wireless Communications, IEEE **11**(1) (Feb 2004) 48–60
18. Roman, R., Lopez, J., Gritzalis, S.: Situation awareness mechanisms for wireless sensor networks. IEEE Communications Magazine **46**(4) (April 2008) 102–107
19. Hugelshofer, F., Smith, P., Hutchison, D., Race, N.J.: Openlids: a lightweight intrusion detection system for wireless mesh networks. In: Proceedings of the 15th annual international conference on Mobile computing and networking. MobiCom '09, New York, NY, USA, ACM (2009) 309–320
20. Giannetsos, T., Krontiris, I., Dimitriou, T., Freiling, F.: Intrusion Detection in Wireless Sensor Networks. In: On Security in RFID and Sensor Networks. Auerbach Publications, CRC Press (2009)
21. Axelsson, S.: Intrusion detection systems: A survey and taxonomy. Technical report, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden (March 2000)
22. Patwari, N., Ash, J., Kyperountas, S., Hero, A.O., I., Moses, R., Correal, N.: Locating the nodes: cooperative localization in wireless sensor networks. Signal Processing Magazine, IEEE **22**(4) (July 2005) 54–69
23. Bucher, R., Misra, D.: A synthesizable vhdl model of the exact solution for three-dimensional hyperbolic positioning system. Vlsi Design **15**(2) (2002) 507–520
24. Foy, W.: Position-location solutions by Taylor-series estimation. IEEE Transactions on Aerospace and Electronic Systems **12**(2) (1976) 187–194
25. Kalman, R., Bucy, R.: New results in linear filtering and prediction theory. Journal of Basic Engineering **83**(3) (1961) 95–108
26. Ureten, O., Serinken, N.: Wireless security through RF fingerprinting. Electrical and Computer Engineering, Canadian Journal of **32**(1) (2007) 27–33
27. Zhengyi, L., Lin, L., Chi, Z.: Fast Detection Method in Cooperative Cognitive Radio Networks. International Journal of Digital Multimedia Broadcasting **2010** (2010)
28. Nieminen, J., Jantti, R., Qian, L.: Primary User Detection in Distributed Cognitive Radio Networks under Timing Inaccuracy. In: New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on, IEEE (2010) 1–8