A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks

Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis

***Abstract*—With the rapid proliferation of new technologies and services in the wireless domain, spectrum scarcity has become a major concern. The allocation of the Industrial, Medical and Scientific (ISM) band has enabled the explosion of new technologies (e.g. Wi-Fi) due to its licence-exempt characteristic. The widespread adoption of Wi-Fi technology, combined with the rapid penetration of smart phones running popular user services (e.g. social online networks) has overcrowded substantially the ISM band. On the other hand, according to a number of recent reports, several parts of the static allocated licensed bands are under-utilized. This has brought up the idea of the opportunistic use of these bands through the, so-called, cognitive radios and cognitive radio networks. Cognitive radios have enabled the opportunity to transmit in several licensed bands without causing harmful interference to licensed users. Along with the realization of cognitive radios, new security threats have been raised. Adversaries can exploit several vulnerabilities of this new technology and cause severe performance degradation. Security threats are mainly related to two fundamental characteristics of cognitive radios: cognitive capability, and reconfigurability. Threats related to the cognitive capability include attacks launched by adversaries that mimic primary transmitters, and transmission of false observations related to spectrum sensing. Reconfiguration can be exploited by attackers through the use of malicious code installed in cognitive radios. Furthermore, as cognitive radio networks are wireless in nature, they face all classic threats present in the conventional wireless networks. The scope of this work is to give an overview of the security threats and challenges that cognitive radios and cognitive radio networks face, along with the current state-of-the-art to detect the corresponding attacks. In addition, future challenges are addressed.**

***Index Terms*—cognitive radios, cognitive radio networks, primary user emulation attacks, spectrum sense data falsification attacks, cross layer attacks, software defined radio security, IEEE 802.22**

I. Introduction

WIRELESS network technology proliferation has been remarkable during the last decade. In 1985, FCC (Federal Communications Commission) [1] issued a mandate defining several portions of the spectrum as ”licence-exempt”. These constitute part of the Industrial, Scientific and Medical (ISM) band where user devices can freely operate without the need of a license.

This visionary mandate, along with the deployment of IEEE 802.11a/b/g standards brought a revolution in the wireless domain. In addition, FCC [2] has also allowed the utilization of additional spectrum for unlicensed devices below 900 MHz, and in the 3 GHz band. Wi-Fi hot-spots offer ubiquitous and inexpensive Internet broadband access to millions of users worldwide. Low-cost IEEE 802.11-compatible devices have been essential parts of desktop and laptop computers, providing anywhere and at anytime Internet access. Furthermore, several metropolitan area wireless networks have been deployed, providing wireless access to thousands of users in large geographical areas. As an example, the Athens Wireless Metropolitan Network [3], built and maintained by volunteers and technology enthusiasts, has more than 1100 nodes providing Internet access to more than 3000 client computers.

The rapid proliferation of wireless technology has spurred the deployment of mesh networks [4]. These are multi-hop wireless networks with enhanced capabilities such as multiple radio interfaces, mechanisms for interference mitigation, self-healing, security, etc., providing multi-Mbps broadband access in large geographical areas with QoS provision.

The demand for Internet access has increased substantially as users’ interests focus continuously on new services such as file transferring through peer to peer networks, and online social network services (e.g. facebook, twitter). This, along with the rapid penetration of smart phones, (according to [5] smart phones in US will overtake feature phones by 2011) will dramatically increase Internet traffic and especially mobile multimedia traffic through 3G infrastructures (mobile broadband), as well as through the existing Wi-Fi enabled networks. As 3G technology cannot satisfy the ever increasing demands for more bandwidth and QoS support of mobile multimedia content traffic, the focus is more on the wireless domain and its support through mesh technologies. These types of technologies can provide multi-Mbps traffic with acceptable QoS.

Nevertheless, as the ISM band is licence-free, it has become overcrowded resulting in increased interference and contention between the networking devices due to the inherent characteristics of the protocols used (IEEE 802.11). Interference and contention are the main reasons for link quality degradation.

Although the ISM band has become overcrowded, there are several (licensed) bands of the spectrum currently being under-utilized. Licensed bands are characterized by the traditional and static allocation process of spectrum assignment, each band serving a distinct service or several channels of a distinct service. For example in US, frequencies from 512-608 MHz have been allocated to TV broadcasting for channels 21-36, while the frequency band from 960-1215 MHz is reserved for aeronautical radio-navigation [6]. There are similar static frequency allocation schemes that differ from country

Manuscript received 13 December 2010; revised 10 June 2011 and 14 September 2011.

A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis are with the Institute of Computer Science of the Foundation for Research and Technology-Hellas (FORTH), P.O. Box 1385, GR 71110 Heraklion, Crete, Greece (e-mail:{alfrag,etragos,asko}@ics.forth.gr.)

Digital Object Identifier 10.1109/SURV.2011.122211.00162

to country. Nevertheless, several studies [7], [8], [9], [10] have shown that parts of the static allocated spectrum are under-utilized. Furthermore, FCC's reference [11] states that temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85%.

A novel idea was proposed by Mitola [12], [13] for the opportunistic use of the under-utilized portions of the spectrum, using novel devices called Cognitive Radios (CRs). When interconnected, CRs form Cognitive Radio Networks (CRNs). CRs are devices that are capable of sensing the spectrum and use its free portions in an opportunistic manner. The free spectrum portions are referred to as "white spaces" or "spectrum holes". A spectrum hole can be formally defined as [14]: ”a band of frequencies assigned to a primary user (PU), but, at a particular time and specific geographic location, the band is not being utilized by that user".

In general, users are divided into two categories: (i) primary or incumbent users[1] that hold a licence for a specific portion of the spectrum, and (ii) cognitive or secondary users (SUs) that use parts of the spectrum in an opportunistic way, so as not to cause harmful interference to PUs. A CR device senses its environment, detects the whites spaces in the spatial and/or temporal domain and decides upon which white space to use. There are several spectrum sensing techniques (energy detection, cyclostationary detection, filter matching, etc.), and various methods for spectrum management and decision (co-operative, distributed, etc.) [15], but these are out of the scope of this paper.

CRNs are expected to bring evolution to the spectrum scarcity problem through intelligent use of the fallow[2] spectrum bands. However, as CRNs are wireless in nature, they face all common security threats found in the traditional wireless networks. In general, due to their open nature, wireless networks are susceptible to several attacks targeting the physical or medium access (MAC) layers. Attacks targeting the physical layer through RF jamming can severely disrupt network's operation as shown in [16], [17]. Attacks at the MAC layer include MAC address spoofing, transmission of spurious MAC frames (e.g. RTS, CTS, ACK) [18], as well as greedy behaviors by cheating on backoff rules [19], [20].

The most common security objectives for wireless networks are [21]: (i) **confidentiality** that ensures that network data cannot be read by unauthorized users, (ii) **integrity** that detects any intentional or unintentional changes to the data occurring in transit, (iii) **availability** that ensures that devices and individuals can access network's resources when needed, and (iv) **access control** that restricts network's resources to authorized individuals or devices only.

Except the previously described threats inherited by their wireless nature, CRNs face new security threats and challenges that have arisen due to their unique cognitive characteristics. Current literature on CRNs describes several approaches for spectrum sensing, spectrum management, and spectrum handoff. Nevertheless, most of these contributions underestimate security issues. However, there is a significant number of contributions that focus especially on CRNs security. These are divided into two main categories: (i) "theoretical" contributions as those described in [22], [23], [24], [25], [26], [27], [28], [29], and (ii) contributions discussing detailed approaches for the detection and mitigation of specific attacks as those in [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47].

A basic operation of the CRs is spectrum sensing. Whenever, a primary signal is detected, CRs have to vacate the specific spectrum band. Malicious users can mimic incumbent transmitters so as to enforce CRs vacate the specific band. This is called as *primary user emulation attack* (PUEA).

Another attack exists that is related to collaborative spectrum sensing, a technique used to improve spectrum sensing in fading environments where multiple CRs collaborate. Here, a malicious CR can provide false observations on purpose. This is called as *spectrum sensing data falsification* (SSDF) attack.

As CRNs are wireless in nature, they inherit all threats present in traditional wireless networks. There are common attacks such as MAC spoofing, congestion attacks, jamming attacks, etc.

IEEE 802.22 [48], [49] is the first standard for enabling the use of the fallow TV bands by infrastructure single-hop CRNs with the presence of one base station (BS) that performs spectrum management. This standard supports the provision of broadband fixed wireless data in sparsely populated rural areas and it has a security mechanism for authentication, data integrity, etc. However, several attacks can be feasible against this mechanism such as the *beacon falsification attack* (BF).

As CRs adopt the layered architecture of the conventional networks, several cross-layers attacks are possible. These can include a combination of a SSDF attack with a small-backoff-window attack (SBW), and the so-called lion attack [50].

CRs are usually based on Software Defined Radios (SDRs), devices with radio functionalities implemented in software. SDRs are vulnerable to a number of software and hardware-related threats.

A detailed analysis of all the above attacks and the corresponding techniques for their detection is the major goal of this work. These attacks are mainly about the availability of the CRNs which is related to DoS attacks. Moreover, most of the described contributions are based on single-hop CRNs with the exception of a couple of contributions described in Section III-C2 that refer to multi-hop CRNs.

The main contributions of this paper are:

- a description of CRs and CRNs in context with the spectrum scarcity and the spectrum under-utilization,
- a categorization and description of the security threats related to the CRs and CRNs,
- an analytical survey of the current state-of-the-art for the detection of the corresponding attacks,
- a discussion of further research challenges.

The remainder of this paper is organized as follows. In Section II the main characteristics of CRs and CRNs are described. In Section III we present the current state-of-the-art on CRs and CRNs threats and attacks, and the corresponding detection techniques. In Section IV we describe future challenges on CRN security. Finally in Section V, our conclusions are presented.

[1] The terms primary and incumbent are used interchangeable throughout the paper

[2] The term fallow is used to characterize the under-utilized or the free spectrum bands

II. Cognitive Radio-A novel solution to spectrum scarcity and spectrum under-utilization

CRs are envisioned as reconfigurable devices that can sense their environment and adapt to any changes accordingly. A formal definition for a CR is [11]: ”*A cognitive radio is a radio that can change its transmitter parameters based on interaction with the environment it operates*”. The goal of a CR is to seek for transmission opportunities in the white spaces and choose the optimal one, in terms of maximizing several utility functions such as users' throughput, fairness, etc., while causing no or minimal interference to PUs.

The research community has made significant efforts towards the standardization of CRNs. IEEE 802.22 [48], [49] is the first standard for enabling the use of the fallow TV bands by infrastructure single-hop CRNs, with the presence of one base station (BS) that performs spectrum management. This standard supports the provision of broadband fixed wireless data in sparsely populated rural areas (it is further analyzed in Section III-C3). ECMA-392 proposed by the European Computer Manufacturers Association (ECMA) [51] is a new standard used by personal/portable devices for exploiting TV-band white spaces. This standard, opposed to IEEE 802.22, targets local area applications in houses, buildings, and neighborhoods. Wi-Fi services through CR operating in TV white bands are the scope of the IEEE 802.11af [52] standard. Furthermore, the European Telecommunications Standards Institute (ETSI) [53] has proposed several standards regarding the Reconfigurable Radio Systems (RRS), systems based on software defined radio and CR technologies. Also, the Wireless Innovation Forum has significantly contributed on the securing of software reconfigurable communications devices [54].

CRs have two main characteristics [55]:

- **Cognitive capability** that makes these devices capable of sensing their environment and choosing the best available transmission mode (e.g. modulation type) in the fallow bands. This becomes feasible through the spectrum management process where several physical layer parameters such as frequency, modulation type, power, etc., are estimated.
- **Reconfigurability** that enables a CR to change several of its parameters (e.g. frequency, modulation, etc.) and adapt to its environment. This is very important as CRs should use the fallow bands in an opportunistic manner, vacating a band (through spectrum hand-off) if any PU transmissions are detected. CRs deployment becomes feasible through the use of the SDRs [56], [57], [58], [59], [60], [61], [62], [63], [64], [65], [66], [67] many of which are equipped with devices with reprogrammable features (e.g. field programmable gate arrays or general purpose processors) that can change their physical layer parameters on-the-fly.

A. Cognitive capability

As mentioned in the previous sections, CR is a device that can sense its environment and adapt accordingly. The operations that a CR performs for adaptive operation are referred to as the cognitive cycle, shown in Fig. 1 [13] (the ellipses shown on this figure are discussed in the next sections). SUs access any of the available spectrum holes opportunistically. If an incumbent signal is detected, SUs have to vacate the specific band immediately.

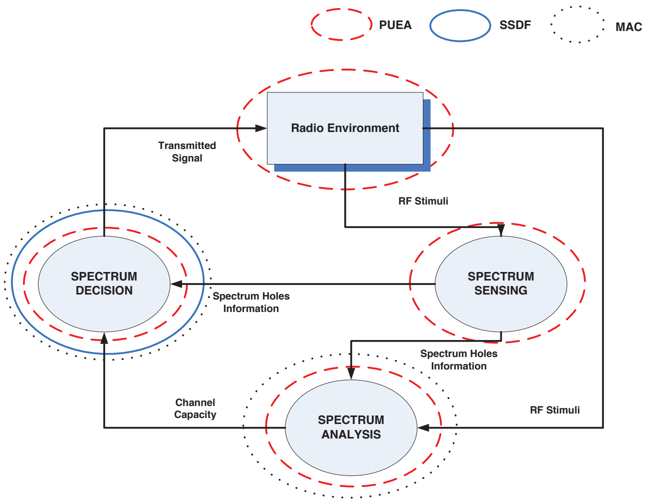

Fig. 1. The cognitive cycle

The cognitive cycle consists of the following mechanisms:

- ***Spectrum sensing***. Incumbent signals' detection is performed during *spectrum sensing* that is one of the most important components of a CR [15]. For example, in IEEE 802.22, there are silent periods, in which all SUs refrain from transmission in order to perform spectrum sensing for the detection of incumbent signals. Two time scales are defined: (i) fast sensing (1ms/channel), and (ii) fine sensing that is dynamically determined by the BS, depending on the output of fast sensing, and its role is to sense the spectrum in more detail. All SUs sense the spectrum and send their observations to the BS that takes the final decision about the incumbent's signal presence or absence. For the detection of the incumbent signal, IEEE 802.22 uses the *energy detection* method because of its simplicity and low computational overhead. This is important as CRs are mobile devices with medium or low computational capabilities and with energy constraints. Except “energy detection”, several other methods have been proposed in the literature such as [15]: (i) waveform based sensing, (ii) cyclostationarity based sensing, (iii) radio identification based sensing, and (iv) matched filtering. An analysis of the advantages and disadvantages of each method is out of the scope of this paper.
- ***Spectrum analysis*** is the process that, based on the available spectrum holes information (feedback from spectrum sensing), analyzes several channel and network characteristics (e.g. bit error rate, capacity, delay) for each spectrum hole. It then feeds the *spectrum decision* process.
- ***Spectrum decision*** is the process which selects the most appropriate spectrum hole for transmission. Spectrum decision can be performed by a single CR, or can be the output of several cooperating CRs.

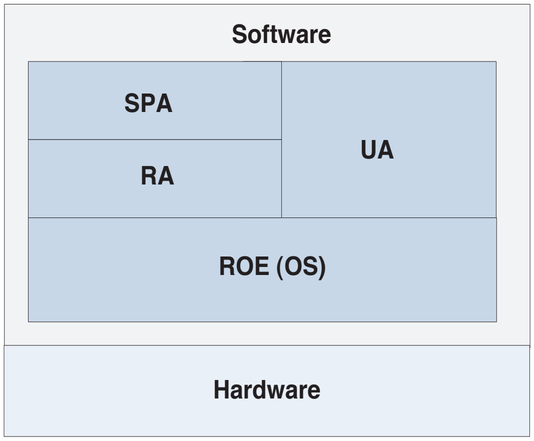

Fig. 2. Software-defined radio architecture

B. Reconfigurability

Reconfigurability is an essential characteristic of CRs that is closely related to their cognitive capability. Reconfiguration of CRs involves the change/modification/update of several characteristics of their physical layer parameters such as: (i) carrier frequency, (ii) type of modulation, (iii) transmission power, etc. CRs have to be flexible and adapt to the environment; therefore physical layer mechanisms purely implemented at the hardware level are not sufficient. SDRs are a viable solution to this concern. These are devices with radio functionality modules implemented in software, providing reconfigurability by using the same equipment in different regions and under different policies (e.g. spectrum regulation enforced by the authorities). In general, a SDR consists of two distinct parts: hardware and software, as shown in Fig. 2. Furthermore, the software part consists of several sub-modules [68]:

- **Radio operation environment (ROE)** contains all the core modules for the radio configuration (e.g. driver, middleware, operating system).
- **Radio applications (RA)** controls the functionality of the radio platform, implementing the air interference and the communication protocols.
- **Service provider applications (SPA)** include services such as messaging, video, voice, etc.
- **User applications (UA)** include all the applications installed by a user (e.g. text editors, web browsers, etc.).

The hardware part of many SDR implementations (e.g. [59], [60], [61], [62], [63], [64], [65], [67], [69]) mainly consists of Field Programmable Gate Array (FPGA) devices [70], [71], because of their high re-programmability, medium-to-high performance (compared to dedicated hardware), and low-energy consumption. Security threats and detection techniques for SDRs are described in Section III-E.

III. Attacks and detection techniques

This section describes the attacks against CRs and CRNs along with the current state-of-the-art techniques to detect them.

A. Primary user emulation attacks

1) Introduction: A fundamental characteristic of a CR is its ability for spectrum sensing, as it shall use the spectrum in an opportunistic manner. This means that the CR has to vacate a currently used spectrum band if an incumbent signal is detected. In this case, CRs perform spectrum hand-off seeking for different spectrum holes for transmissions. Performing spectrum hand-off very often results in degradation of the CR performance since more time for sensing of the spectrum is required, and this decreases the available time for accessing the spectrum. This inherent operation of CRs can be exploited by adversaries that mimic incumbent signals. Nodes launching PUEAs can be of two types:

- **Greedy** nodes that by transmitting fake incumbent signals force all other users to vacate a specific band (spectrum hole) in order to acquire its exclusive use.
- **Malicious** nodes (adversaries) that mimic incumbent signals in order to cause Denial of Service (DoS) attacks. Malicious nodes can cooperate and transmit fake incumbent signals in more than one band, thus causing extensive DoS attacks making a CRN hop from band to band, severely disrupting its operation. Furthermore, adversaries could also cause DoS attacks to PU networks by creating harmful interference. As this actually concerns attacks against PUs, it is out of the scope of this paper.

Regardless the type of the misbehaving node (greedy or malicious), the consequences to a CRN are the same: operation disruption and unfairness among the nodes. Referring to the cognitive cycle, shown in Fig. 1, a PUEA can affect all of its parts as shown by the corresponding dotted ellipses. Initially, PUEAs affect the Radio Frequency (RF) environment by "polluting" it with fake incumbent signals. An immediate effect of RF pollution is a cascading phenomenon affecting spectrum sensing, analysis, and decision. Generally, a CR tries to detect incumbent transmissions using one of the methods described in Section II-A. Energy detection is the most widely method used because of its simplicity and low computational overhead [72], [73], [74], [75]. Nevertheless, this is the most vulnerable method to PUEAs because it does not perform well in low SNR environments. Furthermore, PUEAs can be launched against CRNs that use energy detection by non-sophisticated adversaries, as the generation of energy levels using an incumbent carrier frequency is a trivial task. A PUEA can be more effective on learning CRs [76], as these radios build a long-term behavior based on their observations from the environment.

2) State-of-the-art for the detection of PUEAs: FCC [1] has stated that: "*no modification to the incumbent signal should be required to accommodate opportunistic use of the spectrum by SUs*". This should be followed by all mechanisms proposed in context with CRNs. Most of the contributions regarding security propose appropriate techniques for the detection of PUEAs, such that no modification of the incumbent signal is necessary. Furthermore, a few contributions assume that the location of the primary transmitters is known. Based on this, we present the corresponding works according to this categorization. Table I summarizes the contributions categorized as:

TABLE I
CONTRIBUTIONS FOR PUEA DETECTION

Contribution	Location-based	Work tested using	Cooperation scheme	Advantages	Disadvantages	FCC mandate followed
Jin et al. [30]	Yes	Simulations	No	Use of analytical models for the received power for attack detection.	**(i)** WSPRT is used that can lead to endless sampling and long sensing times, and it may not perform properly in a highly dynamic environment, **(ii)** the assumption that legitimate users and malicious users are uniformly distributed, **(iii)** the assumption that malicious users use constant transmission power.	Yes
Jin et al. [32]	Yes	Simulations	No	**(i)** The fading characteristics of the wireless environment are taken into account, **(ii)** multiple malicious users are considered.	**(i)** the use of an exclusive distance from a cognitive user, **(ii)** the assumption that legitimate users and malicious users are uniformly distributed, **(iii)** the assumption that malicious users use fixed transmission power.	Yes
Chen et al. [35]	Yes	Simulations	Yes	A separate sensor network is used for PUEA detection so cognitive users are not burdened with detection duties.	**(i)** the separate sensor network increases the deployment and maintenance costs, **(ii)** RSS is used that is very volatile, **(iii)** attackers are assumed to use fixed transmission power.	Yes
Liu et al. [34]	No	Simulations and real implementation	No	**(i)** Use of a novel physical layer authentication technique, **(ii)** use of a lightweight authentication protocol.	An extra node (helper node) is needed for every primary transmitter.	Yes
Chen et al. [31]	No	Simulations	No	**(i)** Attackers with a variable transmission power are also considered, **(ii)** the detection method proposed can be used regardless the type of sensing.	**(i)** The position of the attacker has to be known in advance, **(ii)** the distances between the PUs, the SUs and the attacker have to be known in advance.	Yes
Mathur et al. [33]	No	N/A	Yes	A lightweight public key cryptography mechanism between PUs and SUs.	**(i)** Modification of the PUs is necessary, **(ii)** the assumption that PUs operate in the digital domain, **(iii)** a certification authority is needed, **(iv)** the proposed mechanism for encryption/decryption has several vulnerabilities that can lead to severe DoS attacks.	No

- **Location-based or non location-based mechanisms.**
- **Works tested using simulations and/or real implementations**.
- **Cooperation or non-cooperation schemes used**.
- **Advantages** gained by the use of a specific contribution.
- **Disadvantages** by the use of a specific contribution.
- **Incumbent signal modification or not**.

a) Location-based contributions

The work in [35] utilizes both the location information of the primary transmitter and the *Received Signal Strength* (RSS) characteristics. This approach consists of three phases: (i) verification of signal characteristics, (ii) received signal energy estimation, and (iii) localization of the transmitter. It mainly focuses on the localization of the transmitter using a method based on RSS measurements collected by a wireless sensor network. Based on the distribution of the RSS values, a decision is made about if the transmitter is an incumbent transmitter or an attacker. Here, the location of the incumbent transmitter has to be known a priori. This information can be available if the incumbent transmitters are i.e. TV towers, as the authors assume, but in other applications such as in future public safety communication networks using CRs, the location of the incumbent transmitters may not be known as these transmitters can be mobile.

Another drawback of this method is the use of RSS. As it is widely known, RSS fluctuations can be large even within small geographical areas for several reasons such as the presence of obstacles, fading, transmission imperfections, etc. Furthermore, the use of the separate sensor monitoring network, on the one hand relieves cognitive users as they do not have to run any PUEA detection algorithm, thus saving valuable resources but on the other hand, it introduces additional deployment and maintenance costs. Finally, the authors make the assumption that the attackers use fixed transmission power; thus they do not consider sophisticated adversaries.

Detection of PUEAs can be based on algorithms that consider the received power measured at the SU interfaces. The authors in [30] use analytical models for the received power using Fenton's approximation and Wald's Sequential Probability Ratio Test (WSPRT). SUs measure the received power on a spectrum band and if it is below a threshold, the spectrum band is considered to be vacant, otherwise they make a decision whether the detected signal was sent by a legitimate primary transmitter or an attacker. Mathematical expressions are derived for the computation of: (i) the Probability Density Function (PDF) of the received power to a SU due to a PU, and (ii) the PDF of the received power to a SU due to malicious users. Then, WSPRT is used to make a decision between two hypotheses (H0: primary transmitter, H1: malicious user).

The simulation results show that when malicious users are too close to the SUs, the false alarm probability is maximized because the total received power from all the adversaries is larger than the received power from the primary transmitter. Also, when the malicious users are too close, the probability of miss detections is maximized for the same reasons. As the distance from the adversaries increases, both probabilities decrease. The authors here assume that the SUs and the malicious users are uniformly distributed and that the PDF of the received signal on any user is the same as that on any other user. Using these assumptions, cooperation between the SUs is not necessary. However, this is unlikely to be the case in a realistic hostile environment where the locations of the users (either legitimate or malicious) can be totally random. In such cases, cooperating schemes for detecting PUEAs can be more effective.

The authors also state that no information regarding the location of the primary transmitter is necessary for their scheme to work. This is controversial to one of their assumptions, that the coordinates of the primary transmitter are fixed and this position is known to all users; thus location information is necessary. A drawback of this work is that WSPRT is used that can lead to endless sampling and long sensing times, and may not perform properly in highly dynamic environments. Moreover, the authors assume that the attacker uses constant transmission power.

The previous work is extended in [32] where the authors compare the approach based on WSPRT with a Neyman-Pearson Composite Hypothesis Testing (NPCHT). The simulation results show that for the same desired threshold on the probability of missing the primary signal, WSPRT achieves a probability of successful PUEA 50% less than when NPCHT is used. Advantages of this work are that they consider multiple malicious users, and they also take into account the fading characteristics of the wireless environment; hence their results can be considered as more accurate than other contributions. However, the authors make the assumption that the malicious users are close to the legitimate users in a distance not smaller than the ”exclusive” distance. Furthermore, they assume that malicious users use fixed transmission power.

The received power measured at SUs is also used in [31]. The authors use a variance detection method comparing it with a naive method that accounts only for the power of the PUs. They differentiate their work from others commenting that in this work attackers may have variable transmit power, adapting it so as to effectively jam the target network. Both the attacker and the defender can apply estimation techniques to obtain the key information regarding the environment from the received signals and use it to design better strategies. The attacker uses a maximum likelihood estimator to infer the transmit power of the PU, and a mean-field approach to generate primary user emulation signals. The SUs use a defense strategy called as the variance detection method to defend against PUEAs. A key observation stated by the authors and used in this method is that an attacker can mimic many characteristics of a PU signal, but it cannot easily emulate the feature of the communication channel.

SUs perform energy detection as this method, according to the authors, has three advantages: (i) it is easily implemented, (ii) a sophisticated attacker can emulate several characteristics of the primary signal such as cyclostationary characteristics and modulation; thus it would be more difficult for a SU to detect the attack when using the matched filter or the cyclostationary spectrum sensing approaches, and (iii) the method proposed here can be extended for the other spectrum sensing methods. They first show how an attacker can defeat a naive detection method that is solely based on the mean value of the received signal. The simulation results show how the variance method outperforms the naive method. Here, the authors assume that the distances between the PU and the SU, the PU and the attacker, and the attacker and the SU, are known in advance. Of course, the assumption of the a priori knowledge of the attacker's location cannot be realistic in a real hostile environment.

b) Non location-based contributions

The authors in [34] state that the channel impulse response can be used to determine whether a primary transmitter changes its location. Generally, the locations of the primary transmitters can be known in advance as these usually are TV towers or cellular BSs with zero mobility. The channel impulse response is referred to as the “link signature”. Their approach uses a “helper node” that is located in a fixed position very close to a primary transmitter. This node is used as a bridge enabling SUs to verify cryptographic signatures carried by the helper node's signals, and then obtain the helper node's link signatures in order to verify the primary transmitter's signals.

The helper node communicates with the SUs only when the PU is not transmitting; therefore it has to sense the channel first to verify that no incumbent transmission is taking place. For this reason, it has to distinguish PU signals from fake signals transmitted by an adversary. The authentication at this phase is performed using the first and the second multi-path components of the received signal at the helper node. The authors show that if the ratio of the multi-path components is over a threshold, transmissions from a PU are correctly identified with high probability, especially when the distance between the PU and the helper node is very short. SUs examine the distance between the link signatures of the received signals and these of the training set sent by the helper node. If the distance is shorter than a threshold, the received signal belongs to a PU, otherwise, it was transmitted by an attacker and it is discarded. The authors also demonstrate a real implementation of the proposed approach using GNU radios [77] and verify some of their simulation results. One of the assumptions authors have made is that the attacker can have a large maximum transmit power several times of that of a PU.

In contradiction to the above methods that follow the FCC mandate, a countermeasure against PUEAs could use a scheme that integrates cryptographic signatures within the incumbent signals, or the use of an authentication mechanism between a primary transmitter and the SUs. Towards that direction, the authors in [33] propose a scheme against PUEAs using public key cryptography. They assume a centralized Dynamic Spectrum Access (DSA) system similar to IEEE 802.22. SUs sense a specific band during quiet periods and report to the BS, which decides if the specific band is free for use. An adversary can exploit the characteristics of this mechanism and transmit during the quiet periods resulting in a DoS attack as the legitimate SUs will continuously refrain from transmitting or move to other bands. However, the adversary can keep causing DoS attacks by performing spectrum handoffs.

The authors in this work propose a public key cryptography mechanism in which a PU attaches a digital signature to the data units it transmits. The digital signature is generated using the PU id, the current time-stamp, and a private key. When the SUs sense that a primary signal (fake or not) is being transmitted in the specific band, they detach the digital signature from the data units and send it (avoiding duplicates) to the (secondary) BS through a control channel. The secondary BS with the aid of a Certification Authority (CA) (that has a pool of the PUs' public keys) verifies if the detected signal belongs to a PU or to an adversary.

A subsequent drawback derived by this part of this method is that a BS can be the victim of a DoS attack when an adversary continuously emits fake signals, and their corresponding signatures are forwarded from the SUs to the BS. As a consequence, the BS has to continuously decrypt and verify packets; thus wasting resources (e.g. memory, CPU, etc.). As a solution for the mitigation of this attack, the authors propose filtering and discarding of the duplicate signatures at the SUs before communicating with the BS. Nevertheless, an adversary can continuously send fake signals with random digital signatures draining not only the resources of the BS but also congesting the control channel; thus making the secondary network completely inoperable.

B. Spectrum sensing data falsification attacks

1) Introduction: Several transmission features such as signal fading, multi-path, etc., can cause the received signal power to be lower of what path loss models have predicted [29]. This leads to undetected primary signals and harmful interference to PUs. There are two types of fading [29]: shadow fading that is frequency independent, and multi-path fading that is frequency dependent. Shadow fading can cause the "hidden node" problem where a SU, although located within the transmission range of a primary network, fails to detect primary transmissions. Fig. 3 shows a primary transmitter, a number of PUs and several SUs. SU1 fails to detect the transmission of incumbent signals because of shadow fading, so it accesses the incumbent frequency band causing harmful interference to PU1.

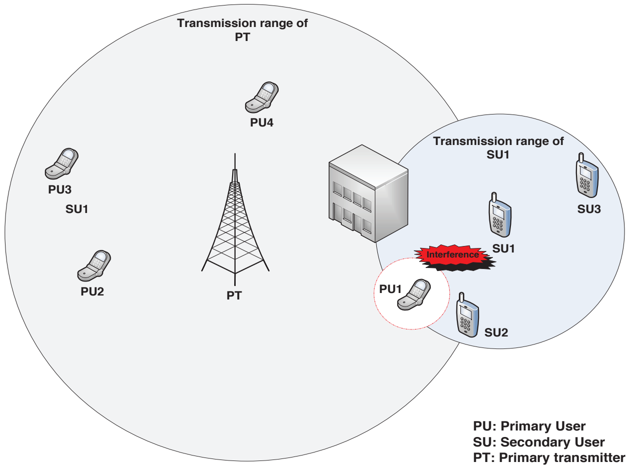

Fig. 3. The hidden node problem

A solution to this problem is the collaborative spectrum sensing technique (see [78], [79], [80], [81], [82], [83], [84], [85]) where a number of users sense the environment and send their observations to a fusion center (FC). FC then fuses the provided information taking the final decision regarding the presence or absent of incumbent transmissions. Another type of sensing is the collaborative distributed sensing where no FC is used. In this case, each SU makes its decision based not only on its observations but also on observations shared by other SUs (e.g. see [86]).

For both types of collaboration, distributed or centralized, SUs have to share their observations or transmit them to a FC. There is always the possibility that one or more SUs send false observations, intentionally or unintentionally. Similarly to PUEAs, nodes sending false observations can be categorized as follows:

- **Malicious** users that send false observations in order to confuse other nodes or the FC. They aim to lead FC or the rest of the nodes to falsely conclude that there is an ongoing incumbent transmission where there isn't, or make them believe that there are no incumbent transmissions when there are. In the first case, the legitimate SUs will evacuate the specific band, while in the second case they will cause harmful interference to the PUs.
- **Greedy** users that continuously report that a specific spectrum hole is occupied by incumbent signals. The goal of these users is to monopolize the specific band by forcing all other nodes to evacuate it.
- **Unintentionally** misbehaving users that report faulty observations for spectrum availability, not because they are malicious or greedy, but because parts of their software or hardware are malfunctioning. The reason for this can be a random fault or a virus [87], [88], [89].

Regardless of the type of the misbehaving users, the reliability of collaborative spectrum sensing can be severely degraded by faulty provided observations. This is called as *Spectrum Sensing Data Falsification* (SSDF) attack. Fig. 4 depicts an example of this type of attack. FC receives observations from SUs and then it decides about the presence or absence of primary transmissions. This type of cooperation can be exploited by malicious users that send malicious reports to the FC on purpose. The authors in [43] show that even a single malicious user can substantially degrade the performance of collaborative sensing. Referring to Fig. 1, SSDF attacks affect the spectrum decision part of the cognitive cycle as faulty observations can lead to faulty decisions.

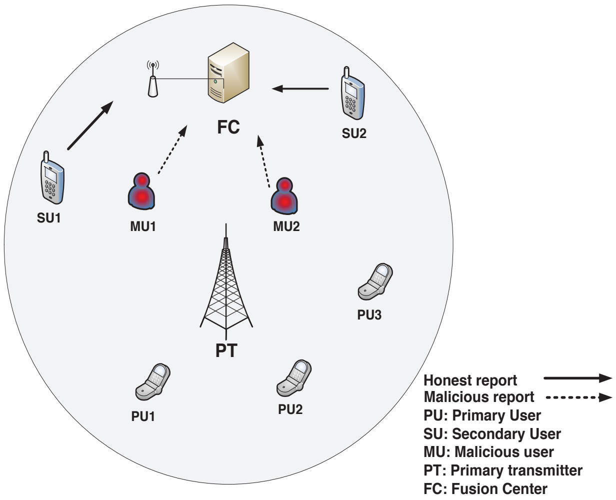

Fig. 4. Spectrum sensing data falsification attack

2) State-of-the-art for the detection of the SSDF attacks: Most contributions for the detection of the SSDF attacks assume a model where a number of SUs sense the environment and report their findings to a FC. In these contributions, opposed to other works related to cooperative sensing (e.g. [78], [79], [80], [81], [82], [83], [84], [85]), SUs are not assumed to be trusted a priori. For this reason, several techniques that compute reputation metrics are introduced aiming to detect and isolate outliers (the term outlier is interchangeable used with adversary and attacker).

After outliers have been isolated, the FC fuses the reports provided by the rest of the nodes. Several fusion rules such as the AND-rule, OR-rule, average-rule, Dempster-Shafer, etc., are used by the FC, depending on the contribution. Furthermore, the reports provided by the SUs can be of two types: (i) continuous (e.g. power estimation from an energy detector) or (ii) binary (e.g. primary transmission is absent/present). Also, some approaches restore the reputation metric of a user if it temporarily misbehaves but after a while it acts legitimately again. Table II summarizes the contributions for SSDF detection categorized as follows:

- **Type of reporting**.
- **Fusion rules used**.
- **Reputation metric restored or not**.
- **Advantages** gained by the use of a specific contribution.
- **Disadvantages** by the use of a specific contribution.

a) Binary type of reporting

In [43] the proposed detection algorithm calculates the trust values of SUs based on their past report. As the authors note, the metric that gives the trust value can become unstable if no attackers are present or there are not enough observation reports. For this reason, they also compute a consistency value for each user. If the consistency value and the trust value fall below certain thresholds, the SU is characterized as an outlier and its reports are not considered for the final decision. For the evaluation of this scheme the authors compare their approach using different fusion rules (OR, K2). They also show how their approach can increase the detection probability and decrease the false alarm rate significantly when the OR rule is used compared to an attack-oblivious method.

A drawback of this work is that only one adversary has been considered. It could be interesting to show how the proposed framework performs as the number of adversaries increases.

The authors in [41] use a reputation metric to detect and isolate attackers from legitimate SUs. For the computation of this metric the output of each SU is compared to the decision made by the FC. If there is a decision mismatch, the reputation metric of the corresponding user increases by one. The smaller the reputation metric is, the more reliable the user is. If the reputation metric of a user exceeds a predefined threshold, its decisions are isolated and thus not used by the FC.

The simulation results show that if the fraction of the number of the attackers over the total number of the SUs (attackers plus legitimate users) is below 0.4, the probability isolation of the attackers can exceed 95%, while the isolation probability of the legitimate nodes is almost zero (FC uses the majority voting rule).

This work is similar to [43] but a key difference is that in [43] they restore the reputation metric if a node temporarily misbehaves and thus this can be regarded as a more fair approach. The temporary misbehavior can be due to reasons related to the location of the user combined with fading (hidden node problem), noise or interference, so the user becomes unaware of the presence of incumbent signals and unintentionally misbehaves. Another drawback of this work is that the reputation metric of a user depends solely on the difference between the observation this user reports and the decision finally made by the FC. This may sound reasonable as majority voting is used for fusion. However, the performance of this scheme could be increased if the reputation metric was based on the past reports of this user as well.

WSPRT is used in [39] for assigning weights to each SU. If the (binary) output of each user is the same with the output produced by FC, the reputation metric of the user is incremented by one, otherwise it is decremented. Opposed to works like [41], if the node temporarily misbehaves, its reputation metric can be restored after a few samples if it starts behaving correctly again.

Each user decides between two hypothesis (incumbent signal present or absent), depending on whether its output is greater or less than two pre-defined thresholds. If it lies between these thresholds, no decision is made and sampling continues; so as opposed to other similar works ([41], [43]), the number of samples can differ depending on the output produced.

For the simulation they assume two attack types: (i) "always true" attackers that always report spectrum to be free, and (ii) "always false" attackers that report the opposite of what they have sensed. Furthermore, eight different data fusion rules are considered for use by the FC. For the "always-false" case the simulation results show that for all fusion rules, except the OR and AND rules, the correct sensing ratio decreases as the number of the attackers increases. For the other two rules, the correct sensing ratio does not vary significantly, but it is lower than the rest of the rules. For the "always-true" case, the results show that the majority rule is substantially affected

TABLE II
CONTRIBUTIONS FOR THE SSDF ATTACK DETECTION

Contribution	**Type of reporting**	**Fusion rules used**	**Reputation metric restored**	**Advantages**	**Disadvantages**
Wang et al. [43]	Binary	OR, K2 and two other proposed schemes	Yes	**(i)** A two-type robust detection scheme that combines the suspicious level and the trustworthiness of the users, **(ii)** the reputation metric is restored, **(iii)** two types of attacks are considered.	Only one adversary is considered.
Rawat et al. [41]	Binary	Majority vote	No	**(i)** Multiple attackers are considered, **(ii)** limits in terms on the fraction of the attackers that can make the FC inoperable are presented.	**(i)** The reputation metric is not restored, **(ii)** the reputation metric depends on the output of the FC that can however be faulty.
Chen et al. [39]	Binary	Majority, AND, OR and five other proposed schemes	Yes	**(i)** Various fusion rules are considered, **(ii)** the reputation metric is restored, **(iii)** multiple attackers are considered, **(iv)** a weighted reputation scheme is used so not all users' observations are treated equally, **(v)** two types of attacks are considered.	WSPRT is used that has several known drawbacks.
Noon et al. [90]	Binary	OR	No	**(i)** A sophisticated attacker with an adaptive strategy is used, **(ii)** the number of the attackers vary.	**(i)** The reputation metric is not restored, **(ii)** it is assumed that the attacker successfully eavesdrops on the other users and the FC.
Li et al. [92]	Binary	OR	N/A	**(i)** Two attack strategies are considered depending on whether the attacker knows the reports sent by the other users, **(ii)** multiple attackers are considered.	SUs are regarded as adversaries if their behavior is very close to that of the correctly behaving users.
Min et al. [40]	Continuous	Weighted Gain Combining	No	**(i)** A realistic two-dimensional shadow-fading field is considered, **(ii)** two types of attacks are presented, **(iii)** multiple attackers are considered.	**(i)** GPS functionalities are required, **(ii)** RSS is used that however has a very volatile nature.
Thanh et al. [38]	Continuous	Dempster-Shafer theory of evidence	Yes	**(i)** The performance of several fusion rules is investigated, **(ii)** multiple attackers are considered, **(iii)** two types of attackers are used.	Dempster-Shafer is used that however has low performance if there are high decision conflicts among the users.
Yu et al. [37]	Continuous	A proposed distributed consensus algorithm	Yes	**(i)** No FC is used, **(ii)** three types of attacks are considered.	A single attacker is considered.
Zhu et al. [36]	Continuous	Two proposed schemes	Yes	**(i)** Two algorithms for attack detection are proposed with a higher performance than WSPRT, **(ii)** three types of attacks are considered, **(iii)** multiple attackers are considered.	A complex algorithm that could introduce significant overhead in limited power devices.

as the number of the attackers increases; therefore this rule is more vulnerable to this type of attack.

The authors in [90] study a specific case of an attacker, the "hit-and-run" attacker. This is an intelligent attacker that, by knowing the fusion technique used by the FC, deviates between an honest mode and a lying mode. The attacker estimates its own suspicious level and as long as it is below a threshold h, it reports faulty observations (lying mode). If its suspicious level drops below a threshold, it behaves legitimately again (honest mode). The detection scheme combines a point system using a similar approach proposed in [91]. When the suspicious level of a node becomes larger than h, a point is assigned to this user. When it exceeds a predefined threshold, the observations of this user are ignored permanently. Simulations show that the proposed scheme achieves good performance for a variable number of attackers (up to three).

A drawback of this method is that a user is permanently removed from a CRN if it collects enough points. However, due to environmental conditions (fading, multi-path, etc.) a user may unintentionally misbehave for a short period of time. An assumption of this work is that an adversary can eavesdrop on other nodes, thus being capable of knowing what other nodes report to the FC. This may not be feasible as strong encryption mechanisms can be available for use in CRN (e.g. IEEE 802.22 security framework).

In [92], a *Double-Sided Neighbor Distance* (DSND) algorithm is used for the detection of outliers. A SU is characterized as an outlier if its reporting to the FC is too far or too close to the reports sent by other users. The authors study two attack modes: the independent attack where an adversary does not know the reports of the legitimate nodes, and the dependent attack where it is aware of what other nodes report. The results show that, in the case of the independent attack, the adversary can always be detected as the number of spectrum sensing rounds tends to infinity. For the dependent attack, the adversary can avoid been detected if it has accurate information about the missed detection and false alarm probabilities.

However, the authors do not give adequate explanations why a SU whose reports are very close to those sent by other users should be characterized as an adversary.

b) Continuous type of reporting

Except the aforementioned contributions that consider binary-type outputs, a number of other contributions use continuous-type outputs. In [42] a scheme for the detection of outliers using a pre-filtering phase based on quartiles is presented. Then, a trust factor is computed over a sample period that identifies more outliers. The performance evaluation shows how this method identifies “always yes” and “always no” nodes, as well as nodes that produce extreme values. For fusion the average rule is used.

An anomaly-based detection method using statistics is described in [40]. A grid of sensors, divided into clusters, send information about their received power (RSS), along with their location to the FC. This approach consists of two phases. First, pre-filtering takes place where possible outliers are isolated and the information they provide is ignored by the FC. During this phase, a per-sample abnormal behavior is detected by examining similarities using the Conditional Probability Density Function (CPDF) of the power for the sensors belonging to the same cluster report. If CPDF lies between two defined thresholds, the SU is characterized as legitimate, otherwise it is tagged as an outlier and its reports are ignored. As the authors note, this pre-filtering step is not adequate in very low SNR environments due to the high sensitivity of the fusion decision to RSS values.

For this reason, a second line of defense follows where a weighted gain combining method assigns weights to the outputs of the sensors based on their CPDF. The FC accumulates the reports sent by all sensors (excluding the users identified as outliers in the pre-filtering phase) and if the total output exceeds a threshold, the frequency band under examination is marked as busy, otherwise it is marked as vacant.

The simulation results show that clustering does not highly affect the incumbent detection if the number of sensors is over twenty. Furthermore, they show how their approach outperforms other similar approaches for detecting outliers. This approach does not restore the reputation of a SU that temporarily misbehaves as it increases a blacklist counter each time the correlation filter’s output does not lie between the defined thresholds. Also, location information provided by the sensors is necessary. For this to become feasible, GPS functionalities or other location verification schemes have to be integrated into the SUs’ equipment, increasing their complexity and cost.

Dempster-Shafer theory of evidence [93] is used by the FC in [38]. Here the authors isolate outliers by using a reputation scheme consisting of two parts. First, a reputation metric is assigned to each SU based on the difference between its output and the final verdict produced by the FC. This metric is then used as a weight for the Dempster-Shafer algorithm executed at the FC. The simulation results show how this approach outperforms other approaches such as the OR and AND fusion rules by increasing the detection probability, while at the same time decreasing the false alarm rate. However, Dempster-Shafer is criticized to have low performance, if there are high decision conflicts among the users (see [94]).

Yu et al. [37] propose a scheme to defend against SSDF attacks in a distributed fashion for cognitive ad-hoc radio networks. A key difference of this work, compared to the rest of the contributions described in this section, is that no FC is used. SUs exchange information and decide independently upon the presence of incumbent transmissions. Each SU applies energy detection to detect the presence of a primary receiver; then it updates its measurements from similar information received by its neighbors, and sends back the updated information. Information sent by potential attackers is filtered out, as each SU computes the maximum deviation of the received information from the mean value. Users with the maximum deviation are assumed to be attackers and their input is ignored later on during the final computation (performed by each user independently). Each user decides that the band under test is occupied if the average result (consensus) (after isolating the information provided by the potential attackers) is greater than a pre-defined threshold. So, the final verdict for each SU depends on the consensus that is computed using its local information, along with that received by the neighboring nodes.

The simulation results show that, with the presence of a single attacker, the estimated PU energy from all SUs is correct and not affected by the attacker. The authors compare their work with the centralized approach proposed in [29], [39], in terms of the false alarm probability. The results show that the distributed consensus approach gives the best results and that the centralized approach is more vulnerable if two attackers are present.

Zhu et al. [36] argue that although WSPRT is a robust method against SSDF attacks, it has several drawbacks:

- **Number of samples**. A large number of samples is required in order to achieve an accepted probability detection rate with low probability of false alarms. Other authors ([39]) have shown that four to five times more samples are necessary compared to the (basic) SPRT method. This means longer sensing times with possible interference to PUs.
- **A possible endless sensing**. WSPRT ends sampling after the output of the FC becomes higher than a threshold or below than another threshold. If it lies in between of these two thresholds, sampling continues. This, under certain network conditions, could lead to a deadlock with no decisions taken and with an endless sensing.
- **Performance issues**. Many parameters of WSPRT, such as the a priori probabilities of the two hypotheses, are fixed, so it may not perform properly in a highly dynamic environment.

The authors propose the Enhanced-WSPRT (EWSPRT) algorithm that has several modifications/improvements compared to WSPRT proposed in [39]. They use a soft decision approach where they differentiate the decisions of the SUs into four categories (strong 1, weak 1, weak 0 and strong 0), whereas the work in [39] adopts a hard decision scheme (0: incumbent signal absent or 1: incumbent signal present). The soft decision approach allows for a better representation of the users’ observations, increasing system’s granularity.

Except the soft decision, they adopt a best of rest strategy where users with high credits (more reliable users) are polled first to submit their decision. This can improve the total sensing delay as EWSPRT can decide on a hypothesis faster than WSPRT that polls users in a random fashion. As WSPRT can lead to a deadlock if network conditions are such that more samples are needed, it eventually leads to an endless sensing. EWSPRT finishes its operation after a maximum number of samples has been used, taking a conservative decision that incumbent signals are present. This conservative decision is to protect PUs from interference. Finally, EWSPRT performs periodic noise measurements that are used to compute the necessary a priori probabilities; thus adapting to dynamic wireless environments with variable fading and multi-path conditions.

A second method proposed by the authors is the *Enhanced Weighted Sequential Zero/One Test* (EWSZOT). This method does not use sequential test like EWSPRT. It collects samples one-by-one and the test is terminated if the difference between the number of reported 1 values and the number of reported 0 values is larger or smaller than two pre-defined thresholds, respectively. WSPRT, EWSPRT and EWSZOT are evaluated using simulations in terms of the false positive rate, false negative rate, correct detection rate, and sampling numbers. The results show that EWSPRT and EWSZOT have better performance than WSPRT, requiring less samples, thus making sensing more secure and faster.

C. MAC layer threats-vulnerabilities and IEEE 802.22 specific threats

1) Introduction: Avoiding interference to PUs is of paramount importance in CRNs, and for this reason the MAC layer is strictly collaborating with the physical layer and the hardware components to accomplish it. Fig. 5 [55] shows the close coupling between the MAC and the physical layers of a CR system. There are several interactions between the layers (cross-layer design), as a CR communication's layout does not follow the strict layer separation of the traditional TCP/IP protocol stack [95].

In general, two types of CR MAC protocols exist [96]: (i) standardized as the IEEE 802.22 protocol, and (ii) application/scenario specific protocols. IEEE 802.22 is a MAC layer protocol for infrastructure-based CRNs, while the application/scenario specific protocols are used in CR ad-hoc networks. CR-MAC protocols for use in distributed CRNs (e.g. [97], [98], [99], [100], [101], [102], [103]), facilitate the deployment of cognitive capabilities without any central entity (e.g. BS) used. A main characteristic of these protocols is the use of a *Common Control Channel* (CCC). As CCC is a critical functionality of a CRN, it can become the target of adversaries aiming to cause DoS attacks. Threats and vulnerabilities regarding CCC are discussed in Section III-C2.

IEEE 802.22 operates in a centralized fashion where several Consumer Premise Equipments (CPEs) sense the environment reporting to a BS that controls and decides upon the access of the available spectrum. As IEEE 802.22 is the first standard for CRNs, its security threats and vulnerabilities are discussed in Section III-C3. In general, the MAC attacks can affect the spectrum decision and analysis parts of the cognitive cycle (Fig. 1).

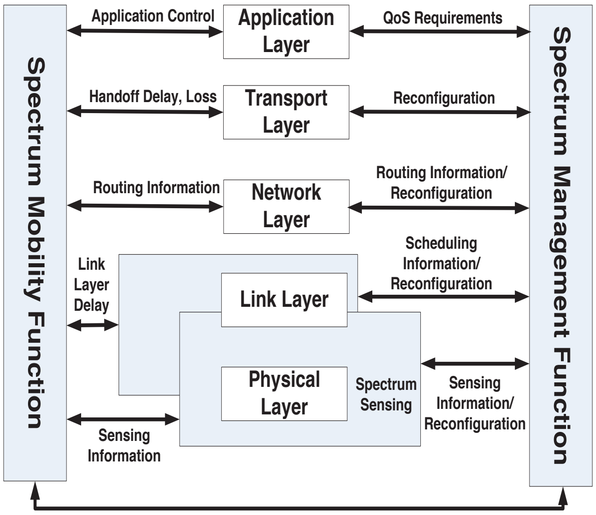

Fig. 5. Cognitive communications layout [55]

2) Common control channel threats and vulnerabilities: CCC plays an important role in enabling CRs to exchange control information. It is an out-of-band channel, which means that the control information and messages are being transmitted using a pre-defined frequency channel, which is different than the one(s) used for exchanging the actual data (that are known as in-band channels). CCC is used for the exchange of several control information regarding for example collaborative sensing, channel negotiation, spectrum hand-off, etc. Protecting the CCC is very important, as this could be the first mechanism that a sophisticated adversary will try to compromise. If he succeeds, network performance will be severely affected since CCC is the main mechanism for controlling the network operations.

The threats that a CCC faces can be categorized as follows:

- **MAC spoofing**, where attackers send spurious messages aiming to disrupt the operation of CRN (e.g. channel negotiation). Multi-hop CRNs are more vulnerable to this type of attack as there is no central entity to control the authentication between the nodes and protect data integrity.
- **Congestion attacks**, where attackers flood CCC in order to cause an extended DoS attack.
- **Jamming attacks**, where attackers cause DoS attacks at the physical layer by creating interference.

The authors in [46], using simulations, show how DoS attacks using spurious MAC frames affect the performance of a multi-hop CRN. The degree of degradation is heavily affected by the number of the attackers. The same work studies the effect on network performance when nodes act selfishly. In a multi-hop CRN, selfish nodes that are located along the path of normal-behaved nodes can drop their packets; thus monopolizing the medium. The results show that with a given topology, Jain's fairness index [104], in terms of throughout, can drop by 20% when the percentage of selfish nodes

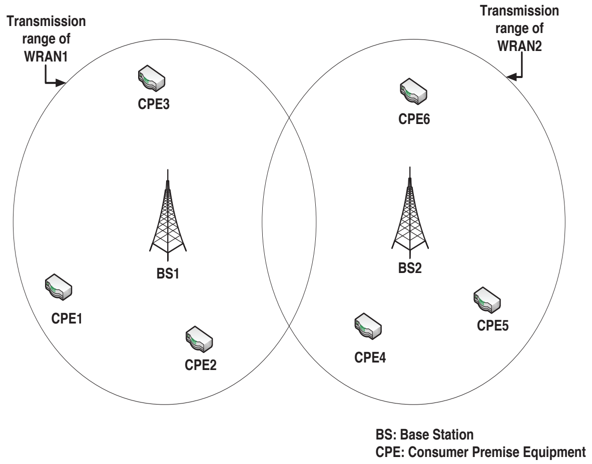
Transmission range of WRAN1
Transmission range of WRAN2
CPE3
CPE6
BS1
BS2
CPE1
CPE2
CPE4
CPE5
BS: Base Station
CPE: Consumer Premise Equipment

Fig. 6. Two overlapping IEEE 802.22 WRANs

becomes more than 25%. Safdar et al. [47] propose a security framework for CCC in multi-hop CRNs where authentication and data integrity take place between a cognitive sender and a cognitive receiver, as well as between their one-hop neighbors.

Jamming attacks [16], [105], [106], [107], [108] are a common problem in the wireless domain. Attackers can emit energy in neighboring channels that the legitimate users operate, creating interference. Interference, as shown in [16], [17], can severely disrupt the network operation.

3) IEEE 802.22 *security threats:* IEEE 802.22 [48], [49] is the first standard based on CR technology. It describes the air interface of a Wireless Regional Access Network (WRAN) for the opportunistic use of the fallow TV bands. Each WRAN consists of a BS and a number of CPEs. BS has the leading role managing CPEs within its WRAN. A WRAN is a point to multi-point network with CPEs placed at fixed locations, with its range varying from 33 to 100 km, depending on the transmitted power. For this reason, WRANs will probably overlap with each other. Fig. 6 shows a typical IEEE 802.22 CRN consisting of two overlapping WRANs.

For the incumbent protection from harmful interference, IEEE 802.22 deploys several mechanisms. CPEs perform distributed sensing, sending their observations to BS that decides upon spectrum use. Two major threats exist here: PUEAs and SSDF attacks. IEEE 802.22 uses energy detection for the detection of incumbent signals. PUEAs can disturb the proper operation of the network. A counter-measure considered by IEEE 802.22 is the combination of the data sent by the energy detectors with geo-location information.

SSDF attacks also pose a significant threat. IEEE 802.22 provides authentication, authorization, message integrity, confidentiality and privacy using a security mechanism derived from IEEE 802.16 [109]. Several parts of the Privacy Key Management Version 1 (PKMv1) along with parts of PKMv2 used in IEEE 802.16 have formed the Secure Control and Management (SCM) protocol used by IEEE 802.22. This is based on a client/server authentication scheme that allows the authentication between the CPEs and BS. Using this security layer, adversaries launching SSDF attacks can be detected and isolated.

As stated in the beginning of this section, multiple WRANs can co-exist and overlap as their transmission range can vary up to 100 km. This overlapping could decrease the overall throughput of WRANs if all used the same spectrum band at the same time. Moreover, overlapping could also decrease the efficiency of spectrum sensing and cause interference to incumbent receivers. To avoid this, cooperation between WRANs has been proposed, referred as self-coexistence (SC). SC aims to minimize interference to incumbent receivers and to increase the performance of WRANs. It consists of two types:

- **Inter-cell synchronization**. IEEE 802.22 (within a WRAN) has defined Quiet Periods (QPs) where spectrum sensing is performed and SUs are not allowed to transmit. WRANs can synchronize their QPs in order to improve spectrum sensing reliability. This is performed through an offset synchronization technique using beacons [110].
- **Inter-BS dynamic resource sharing**. During the network operation of a WRAN, several QoS constraints may not be met with the current channel used. In this case, the specific BS can decide to switch to a different channel (spectrum handoff). The candidate channel may be currently in use by a different WRAN. There are two types of inter-BS dynamic resource sharing [110]:
  - **non-exclusive spectrum sharing**, where the BS performs a spectrum handoff to a new channel and measures the SIR (Signal-to-Interference ratio). If the SIR is higher than a threshold permitting proper network operation, the BS schedules all transmissions using this channel. If the SIR is lower than the required SIR threshold, then exclusive spectrum sharing is triggered.
  - **exclusive spectrum sharing**. Here the *On-Demand Spectrum Contention* (ODSC) protocol is used. The BS that seeks for a new channel to operate randomly selects a *Channel Contention Number* (CCN) that is uniformly distributed in $[0, W]$, where W is the contention window size. The selected CCN is attached to a beacon frame broadcasted so other BSs belonging to different WRANs can detect it. Each BS that receives the beacon and operates on the same channel chooses its CCN from the same contention window. The winner of this contention is the BS with the highest CCN.

Security threats raise when malicious users send spurious beacons aiming either to disrupt synchronization between BSs during QPs, or to disrupt exclusive spectrum sharing. The disruption of synchronization can decrease the reliability of spectrum sensing; hence increasing the probability of secondary transmissions while incumbent transmissions are taking place, causing harmful interference to incumbent receivers. Disruption of the exclusive spectrum sharing is feasible through transmission of spurious beacons that contain very large CCN values by an adversary. This is called as the *Beacon Falsification* (BF) attack [110].

The authors in [110] use an adversary that chooses CCN values from the range $[W/z, W]$, where $z \geq 1$. They show that the probability that the adversary selects the target channel

TABLE III
IEEE 802.22 SECURITY THREATS

Type of attack	Mechanism for attack prevention/detection
Primary User Emulation Attacks	combining the observations sent by the CPEs with geo-location information
Spectrum Sense Data Falsification Attacks	the Secure Management Protocol (authentication scheme)
Beacon Falsification Attacks	a beacon authentication mechanism (optional)

instead of other k contending destinations (BSs) is: $p_w = (p_p)^k = (\frac{z+1}{2z})^k$.

BF attacks, as well as attacks aiming to disrupt the synchronization during QPs, are addressed by IEEE 802.22 using an optional authentication mechanism. Beacons are signed using public key cryptography and the signature is added in the beacon frame. The destination BSs verify the signature using the public key of the BS that transmitted the beacon. If the signature is verified, the ODSC protocol is triggered, otherwise the beacon is dropped. Table III summarizes the threats for IEEE 802.22 networks and the mechanisms used for their prevention/detection.

D. Cross-layer attacks

In the previous sections the presented threats and detection contributions focused only on single-layer measurements and techniques. PUEAs and SSDF attacks focus on the physical layer of a CRN. MAC threats, as well as specific threats for the IEEE 802.22 CRNs focus on the MAC layer. However, adversaries can launch attacks targeting multiple layers. These are called as "cross-layer" attacks and can affect the whole cognitive cycle (Fig. 1), as attacks at all layers become feasible.

In [111] the authors launch two types of attacks against a CRN: SSDF attacks and Small-Backoff-Window (SBW) attacks. SBW is a very common attack in wireless networks where malicious users choose a very small value for minimum Contention Window (CWmin) (e.g. see [112], [113], [114]) aiming to monopolize bandwidth. SBW attacks are feasible against CRs with MAC layers using a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) type of access. Several MAC protocols designed for CRNs are of this type [96].

In [111] two distinct mechanisms for the detection of cross-layer attacks are used: (i) a hypothesis testing scheme residing at the physical layer to detect SSDF attacks, and (ii) a detection scheme residing at the MAC layer aiming to detect adversaries by observing the distribution of the backoff window size and comparing it with the expected (real) distribution. For each layer (and for each node), a trust value is computed that is further fused by a central node. Using simulations, SSDF and SBW attacks are created with probabilities P1 and P2, respectively. The authors compare the performance of the cross-layer detection scheme with a scheme that executes independently at the MAC and physical layers. The results show that the cross-layer detection scheme has superior performance.

In [50] the authors show how a PUEA or a SSDF attack can propagate up to the transport layer and degrade the performance of TCP connections. This type of attack, named as *lion attack*, forces legitimate nodes to perform spectrum handoff mostly by mimicking incumbent signals. In general, TCP uses a retransmission timer (RTO) for each transmitted data segment. If RTO expires without receiving an acknowledgment from the receiver, TCP flags the segment as lost due to congestion and it is retransmitted, while the congestion window reduces to one segment; thus throughput reduces. As TCP is completely unaware of the current status at the physical layer (spectrum handoff), the lion attack can dramatically reduce its throughput by exploiting this vulnerability.

For the mitigation of this attack the authors provide very general recommendations such as: making TCP layer aware of the cognitive capability of CRs so it acquires information from the physical layer, and securing the operation of a CCC for channel negotiations during the attack.

E. Software-defined radio security

As mentioned in Section II-B, SDRs are of major importance for the realization of CRs as they can provide on-the-fly reconfigurability; hence their protection against attacks or malfunctioning is of paramount importance. SDR security protection falls into two main categories: software-based protection, and hardware-based protection.

Software-based protection schemes involve the deployment of tamper-resistance techniques to defend against malicious or buggy software installations. These schemes also involve techniques and algorithms for the secure download and distribution of software into several SDRs. As CRNs have to be flexible, updated software can be frequently downloaded from servers through the Internet. Secure downloading involves mechanisms that protect the integrity of the data exchanged, protect against eavesdropping, as well as providing secure authentication between the communication parties. Pieces of software code that can be updated are shown in Fig. 2 where an abstract view of a SDR is depicted.

Hardware-based protection schemes include modules implemented in hardware acting as isolation layers between hardware and the software components. These modules monitor several parameters of the SDR (e.g. transmission power).

Brawerman et al. [115] propose the *Light Secure Socket Layer* (LSSL) protocol that securely connects SDR devices with software servers maintained by the manufacturers. This is based on Secure Socket Layer (SSL), but it requires less bandwidth than SSL, thus being suitable for resource-constraint devices. The proposed framework, besides LSSL, employs mechanisms for mutual authentication, public/private key data encryption and data integrity checking through fingerprint calculations. Using Java, the authors show how LSSL outperforms SSL.

[116] describes a secure downloading system that uses the characteristics of FPGAs, hosted in a SDR. The connections between the configuration logic blocks (fundamental units of FPGAs) can be arranged in many ways; thus enabling high security encipherment. The authors show that their proposed scheme has high immunity against illegal acquisition of software through replay attacks.

The authors in [117] propose a hardware-based method where the maximum transmission power is computed and controlled by a module implemented at the hardware level of the SDR transceiver. The advantage is that the module, which estimates the maximum transmission power, is isolated from the software layers, which can either be compromised more easily by attackers or malfunction due to software bugs. The authors assume that SUs access the spectrum in an overlay approach; thus secondary and primary transmissions can take place at the same time. The overlay approach can increase the capacity of the secondary network, but it can also cause interference to the primary network [118]. The maximum power of a secondary transmitter is estimated by taking into account the minimum SNR of the primary network for proper operation.

In [88] the authors propose the use of a *Secure Radio Middleware* (SRM) layer, which is purely implemented in software and resides between the operating system and the hardware. Its role is to check all software requests sent to the hardware layer for operations regarding transmission power, frequency, type of modulation, etc. All requests are checked against a policy database, and non-conforming requests are discarded. Security policies can be provided by dedicated policy servers, by other SUs, or primary transmitters.

A prototype of SRM has been implemented using VmWare [119] and the GNU Radio toolkit. The experimental results show that the overhead incurred is small and tolerable. However, as the authors state, the overhead has been estimated in a testbench with generously available resources; thus their proposed framework overhead may be significant if integrated with resource constraint devices (e.g. mobile phones). A light weight solution is proposed with the use of Microkernel [120].

A tamper resistance technique for the protection of SDR software is described in [89]. This approach utilizes code encryption and branch functions, obfuscating the target software. They authors employ a technique called *Random Branch Function Call* (RBFC), consisting of two phases: (i) transformation where the unprotected assembly code becomes tamper-resistance protected offline, and (ii) verification where a code is checked for integrity violations. The proposed scheme is designed to thwart static attacks (static information extracted by examining the software code) and to protect partially against dynamic attacks (dynamic information extracted while the software code executes).

Experiments were performed using GNU Radio and the SPECINT2006 benchmark suite [121]. The performance evaluation shows that when the proposed approach is used: (i) the file size increases no more than 4.5%, (ii) the runtime overhead is less than 4.7%, (iii) the end-to-end delay is heavily affected by the hash computations of this method (its contribution is more than 57.7%), and (iv) the end-to-end delay increase can affect the impact on voice quality (computed by using the subjective voice quality measurement technique R-factor [122]).

The authors in [123] highlight the importance of user authentication in a SDR system. They propose a security architecture that can employ biometric sensors and processors for authentication based on users' traits such as voice, fingerprint, etc. However, the proposed scheme has not been implemented or tested.

Michael et al. [124], [125], [126] describe an approach that combines the employment of a tamper-resistant hardware and four cryptographic methods: (i) secret key encryption, (ii) public key encryption, (iii) digital signature, and (iv) cryptographic hashing. Terminal keys are securely stored in the tamper-resistant hardware and software is distributed using a hardware maker.

In [127] a framework for cloning prevention of SDR Mobile Devices (SDR-MD) is presented. It provides a set of software and hardware technologies that along with the cooperation of a Wireless Operator (WO) can prevent cloning. The WO in this contribution is assumed to be the manufacturer of the SDR. The cooperation is performed through an authentication process where the WO verifies that the specific SDR is the original and not a cloned one. The proposed framework is independent of the communication protocol used, so it can be deployed for mobile devices (e.g. 3G), as well as for Internet technologies (e.g. IEEE 802.11).

SDR security is of paramount importance. A compromised or misbehaving SDR can affect all parts of the cognitive cycle (Fig. 1), as PUEAs, SSDF, and MAC attacks are feasible. An attacker that takes control over an SDR can launch combinations of several attacks. For example, it can provide wrong observations to a FC (SSDF attack), and at the same time it can mimic a primary transmitter (PUEA). This type of adversary poses a greater threat as its attack is amplified by the combination of several other attacks. An interested reader could further refer to [128] where a survey for CRs focusing on SDR is described.

IV. Discussion-Future challenges

Security threats that raise from the use of cognitive technology fall into two categories: threats to PUs, and threats to cognitive users. An important requirement for cognitive users is that they should access the licensed spectrum on an non-interfere basis in order to avoid interfering with PUs. Nevertheless, malicious cognitive users can cause severe DoS attacks in primary networks through interference. As this actually falls within security threats to primary networks, is out of the scope of this paper.

The second category of security threats are those related to CRNs and the respective attacks against them. Table IV summarizes the attacks against CRNs. Denial of Service attacks are very challenging to thwart in CRNs. There are new vulnerabilities that can be exploited by potential attackers leading to effective spoofing and integrity attacks, affecting both spatial (in a large geographic area, e.g. using wide range TV signals with IEEE 802.22 technology), and temporal (that last over time) behavior of the network. As shown in this paper, there is lately much interest regarding security in CRNs.

TABLE IV
ATTACKS AGAINST COGNITIVE RADIO NETWORKS

Type of attack	Layer referred	Main characteristic
Primary user emulation attack (PUEA)	Physical	Emulation of primary transmitters' signal
Spectrum sense data falsification (SSDF) attack	Physical	Provision of wrong observations regarding spectrum sensing
Common control channel (CCC) attacks	Medium access	Targeting CCC through MAC spoofing, congestion attacks, jamming attacks
Beacon falsification (BF) attack	Medium access	Disruption of synchronization between IEEE 802.22 WRANs
Cross layer attacks	All layers	Sophisticated attacks targeting multiple layers
Software defined radio (SDR) attacks	All layers	All above attacks through software or hardware tampering of SDRs

Many techniques for PUEA detection have been investigated and most of them assume that CRs use the energy detection technique for spectrum sensing. Although energy detection is the most widely used spectrum sensing technique, it cannot provide reliable results because of the uncertainty of the noise level in very dynamic environments. Thus, new security techniques based on other spectrum sensing methods like matched filter detection, and cyclostationary feature detection should be investigated.

Specifically, regarding matched filter detection where the signal of the primary transmitter is supposed to be known a priori, malicious users can transmit a signal that matches the modulation type and order, the pulse shape and the packet format of the primary signal. This aims to force the rest of the users to evacuate the specific band so as not to cause harmful interference to PUs. An example is the TV signals for which no authentication mechanism exists. An adversary by exploiting this vulnerability can generate and transmit signals that mimic TV signals, closely to an IEEE 802.22 WRAN. This will force BSs to decide spectrum hand-off, evacuating the currently used band.

A very common requirement of the proposed contributions regarding the detection of PUEAs, is that the locations of primary transmitters are known a priori. This assumption holds in the case of IEEE 802.22 CRNs where the location of the TV transmitters can be known in advance as they have zero mobility. Apart from TV transmitters considered in IEEE 802.22, other types of primary transmitters like BSs of the current mobile networks exist. Updated records regarding the locations of these stations may not be possible as more transmitters can be added in order to increase coverage. For example, the location of the Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS) BSs of the different operators can be possibly unknown because mobile operators are reluctant to publish such information in order not to raise health concerns among the population; therefore, the assumption that primary transmitters' locations are known a priori is simplistic and mainly unrealistic.

For this reason, more advanced techniques that do not assume a prior knowledge of primary transmitters' locations should be investigated in the future. This is necessary because the rapid proliferation of new technologies, such as WiMAX [129], will: (i) increase the number of the primary transmitters, and (ii) their location might not be known in advanced; therefore, non-advanced algorithms that require a priori knowledge of the primary transmitters' locations will have low performance in detecting PUEAs.

Most techniques for the detection of SSDF attacks consider a centralized entity (BS or FC) that collects observations and decides upon the absence/presence of incumbent signals. These techniques exploit the advantages of cooperative spectrum sensing where a number of users exchange messages with the FC. The advantage of using this centralized scheme is that malicious reports can easily be detected and discarded. However, a major disadvantage of this method is that the FC can become a single point of failure if successfully attacked by adversaries. An adversary can cause severe DoS attacks (e.g. through jamming) to the FC making the whole CRN completely inoperable. Furthermore, malfunctions or random failures (e.g. electricity black-out) of the FC will also disrupt the CRN operation completely.

For these reasons more sophisticated algorithms should be investigated, allocating FC responsibilities to more than one SU. A possible solution could be an intelligent clustering scheme where SUs are grouped into clusters. Using this scheme, different clusters can be controlled by different FCs and if a FC becomes inoperable, its associated (managed) nodes will join a different cluster.

As CRNs are wireless in nature, they face all common threats present in conventional wireless networks (jamming, etc.). Sophisticated adversaries can combine classic attacks with attacks specific for CRNs. For example, an attacker that has compromised a legitimate IEEE 802.22 CPE or has by-passed the authentication/authorization process of this standard can be aware of the sensing periods and generate spurious signals in the vicinity of the CRN during the periods that are dedicated for spectrum sensing. So, he can:

- **Generate noise** during the sensing periods only when a primary signal is present. This could lead to undetected primary signals by the CRs and possible interference to the incumbent transmitters if CRs decide to transmit as they assume spectrum is vacant.
- **Mimic incumbent signals** during the sensing periods only when a primary signal is absent. This can be regarded as an advanced PUEA.

To the best of our knowledge there are no contributions studying such types of attacks.

V. Conclusion

The proliferation of wireless network technology has been remarkable in the last decade. The demand for Internet traffic through wireless infrastructures has increased substantially due to the widespread use of smart phones, the popularity of several online services (e.g. social networks), and the reduced subscription costs. An immediate effect of this increase is the overcrowding of the ISM band.

On the other hand, several portions of the licensed spectrum are under-utilized. Towards providing solutions to these shortcomings and meeting the ever increasing user demands, new technologies for future networks are investigated and proposed. A promising technology is the CRNs where CRs can access the under-utilized spectrum in an opportunistic manner. However, CR technology raised new threats and vulnerabilities because of its two fundamental characteristics: cognitive capability, and reconfigurability. Moreover, as CRNs are wireless in nature, they face all common threats present in traditional wireless networks (e.g. IEEE 802.11).

This paper presented the most important contributions on security threats and detection techniques, describing their advantages and shortcomings. In addition, new challenges and directions for future research were discussed.

References

[1] FCC, 1985, authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations. Federal Communications Commission. June 18, 1985. http://www.marcus-spectrum.com/documents/81413RO.txt.

[2] ——, 2002, eT Docket No 02-328 Additional Spectrum for Unlicensed. Devices Below 900 MHz and in the 3 GHz Band, December 2002.

[3] "Athens wireless metropolitan network, http://en.wikipedia.org/wiki/Athens_Wireless_Metropolitan_Network."

[4] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Comput. Netw. ISDN Syst.*, vol. 47, no. 4, pp. 445–487, 2005.

[5] "Nielsen wire, http://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011/."

[6] "United states frequency allocations, http://www.ntia.doc.gov/osmhome/allochrt.pdf."

[7] M. Islam, C. Koh, S. Oh, X. Qing, Y. Lai, C. Wang, Y. Liang, B. Toh, F. Chin, G. Tan, and W. Toh, "Spectrum Survey in Singapore: Occupancy Measurements and Analyses," in *Proc. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2008, pp. 1–7.

[8] V. Valenta, Z. Fedra, R. Marsalek, and M. Villegas, "Analysis of spectrum utilization in suburb environmentevaluation of potentials for cognitive radio," in *Proc. Ultra Modern Telecommunications and Workshops, ICUMT 2009*, 2009, pp. 1–6.

[9] K. Qaraqe, H. Celebi, A. Gorcin, A. El-Saigh, H. Arslan, and M. Alouini, "Empirical results for wideband multidimensional spectrum usage," in *Proc. 20th IEEE Personal, Indoor and Mobile Radio Communications, 2009*, 2009, pp. 1262–1266.

[10] M. Wellens and P. Mahonen, "Lessons learned from an extensive spectrum occupancy measurement campaign and a stochastic duty cycle model," in *Proc. TridentCom 2009*, 2009, pp. 1–9.

[11] FCC, 2003, eT Docket No 03-222 Notice of proposed rule making and order, December 2003.

[12] J. Mitola, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE International Workshop on Mobile Multimedia Communications (MoMuC)*, 1999, pp. 3–10.

[13] ——, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D. dissertation, KTH Royal Institute of Technology, 2000.

[14] P. Kolotzy, "Next generation communications: Kickoff meeting," in *Proc. DARPA*, 2001.

[15] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tutorials*, vol. 11, pp. 116–130, 2009.

[16] A. Fragkiadakis, V. Siris, and N. Petroulakis, "Anomaly-based intrusion detection algorithms for wireless networks," in *WWIC 10*.

[17] A. Fragkiadakis, E. Tragos, T. Tryfonas, and I. Askoxylakis, "Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype," *EURASIP Journal on Wireless Communications and Networking*, to appear in 2012.

[18] M. Thamilarasu, S. Mishra, and R. Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad hoc networks," in *Proc. Milcom '06*, 2006, pp. 1–7.

[19] M. Raya, J. Hubaux, and I. Aad, "Domino: A system to detect greedy behavior in ieee 802.11 hotspots," in *Proc. MobiSys '04*, 2010, pp. 1–8.

[20] A. Cardenas, S. Radosavac, and J. Baras, "Evaluation of detection algorithms for mac layer misbehavior: Theory and experiments," *IEEE/ACM Trans. Netw.* , vol. 17, pp. 605–617, 2009.

[21] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, 2007, establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, NIST Special Publication 800-97.

[22] S. Sanyal, R. Bhadauria, and C. Ghosh, "Secure communication in cognitive radio networks," in *Proc. Computers and Devices for Communication (CODEC)*, 2009, pp. 1–4.

[23] T. Brown and A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment," in *Proc. CrownCom*, 2007, pp. 456–464.

[24] T. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," in *Proc. CrownCom*, 2008, pp. 1–8.

[25] J. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in *Proc. CrownCom*, 2008, pp. 1–7.

[26] S. Arkoulis, G. Marias, P. Frangoudis, J. Oberender, A. Popescu, M. Fiedler, H. Meer, and G. Polyzos, "Misbehavior scenarios in cognitive radio networks," *Future Internet*, vol. 2, no. 3, pp. 212–237, 2010. [Online]. Available: http://www.mdpi.com/1999-5903/2/3/212/

[27] A. Sethi and T. Brown, "Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks," in *Proc. DySPAN*, 2008, pp. 1–7.

[28] N. Prasad, "Secure Cognitive Networks," in *Proc. EuWiT*, 2009, pp. 107–110.

[29] R. Chen, J. Park, T. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, pp. 50–55, 2008.

[30] Z. Jin and K. Subbalakshmi, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in *Proc. ICC*, 2009, pp. 1–5.

[31] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. of IPCCC*, 2009, pp. 208–215.

[32] Z. Jin, S. Anand, and K. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," in *Proc. ACM SigMobile Computing and Communication Review*, 2009, pp. 74–85.

[33] C. Mathur and P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proc. 1st IEEE Workshop on Cognitive Radio Networks*, 2007, pp. 1037–1041.

[34] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in *Proc. 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 286–301.

[35] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.* , vol. 26, pp. 25–37, 2008.

[36] F. Zhu and S. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," *Journal of Communications and Networks*, vol. 11, pp. 122–133, 2009.

[37] F. Yu, M. Huang, Z. Li, and P. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *Proc. Milcom*, 2009, pp. 1–7.

[38] N. Nhan and I. Koo, "An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context," *IEEE Commun. Lett.*, vol. 13, pp. 492–494, 2009.

[39] R. Chen, J. Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in *Proc. Milcom*, 2008, pp. 1876–1884.

[40] A. Min, K. Shin, and X. Hu, "Attack-tolerant distributed sensing for dynamic spectrum access networks," in *Proc. ICNP*, 2009, pp. 294–303.

[41] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Countering byzantine attacks in cognitive radio networks," in *Proc. ICASSP*, 2010, pp. 3098–3101.

[42] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," in *Proc. ICC*, 2008, pp. 3406–3410.

[43] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. CISS*, 2009, pp. 130–134.

[44] L. Zhu and H. Zhou, "Two types of attacks against cognitive radio network mac protocols," in *CSSE (4)*, 2008, pp. 1110–1113.

[45] Y. Tan, S. Sengupta, and K. Subbalakshmi, "Coordinated Denial-of-Service Attacks in IEEE 802.22 Networks," in *Proc. ICC*, 2010, pp. 1–5.

[46] K. Bian and J. Park, "MAC-layer misbehaviors in multi-hop cognitive radio networks," in *Proc. UKC*, 2006, pp. 1–8.

[47] G. Safdar and M. O. Neill, "Common Control Channel Security Framework for Cognitive Radio Networks," in *Proc. VTC*, 2009, pp. 1–5.

[48] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "Ieee 802.22: An introduction to the first wireless standard based on cognitive radios," *Journal of Communications*, vol. 1, pp. 38–47, 2006.

[49] C. Stevenson, G. Chouinard, W. Hu, S. Shellhammer, and W. Caldwell, "Ieee 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol. 47, pp. 130–138, 2009.

[50] J. Hernández-Serrano, O. León, and M. Soriano, "Modeling the lion attack in cognitive radio networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, p. 10 pages, 2011.

[51] J. Wang, "First cognitive radio networking standard for personal/portable devices in tv white spaces," in *DySPAN*, 2010, pp. 1–12.

[52] "Mac and phy proposal for 802.11af, https://mentor.ieee.org/802.11/dcn/10/11-10-0258-00-00af-mac-and-phy-proposal-for-802-11af.pdf."

[53] "The european telecommunications standards institute, http://www.etsi.org/."

[54] "Wireless innovation forum security working group, reconfigurable communications devices, winnf-08-p-0013."

[55] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks Journal (Elsevier)*, vol. 50, pp. 2127–2159, 2006.

[56] E. Jones, "Software Defined Radios, Cognitive Radio and the Software Communications Architecture (SCA) in relation to COMMS, radar and ESM," in *IET Seminar on Cognitive Radio and Software Defined Radios: Technologies and Techniques, September*, 2008, pp. 1–7.

[57] A. Bourdoux, J. Cranickx, A. Dejonghe, and L. Perre, "Receiver Architectures for Software-defined Radios in Mobile Terminals: the Path to Cognitive Radios," in *IEEE Radio and Wireless Symposium*, 2007, pp. 535–538.

[58] F. Jondral, "Software-defined radiobasics and evolution to cognitive radio," *IEEE Commun. Surveys Tutorials*, vol. 3, pp. 116–130, 2005.

[59] "Ettus research, usrp products, http://www.ettus.com/products."

[60] C. Chen, "Reconfigurable software defined radio and its applications," *Tamkang Journal of Science and Engineering*, vol. 13, pp. 29–38, 2010.

[61] F. Ge, "Cognitive Radio: From Spectrum Sharing to Adaptive Learning and Reconfiguration," in *IEEE Airospace Conference*, 2008, pp. 1–10.

[62] H. Harada, "A small-size software defined cognitive radio prototype," in *PIMRC*, 2008, pp. 1–5.

[63] G. Minden, "KUAR: A Flexible Software-Defined Radio Development Platform," in *Proc. DySPAN*, 2007, pp. 428–439.

[64] P. Amini, E. Azarnasab, S. Akoum, and B. Farhang-Boroujeny, "An Experimental Cognitive Radio for First Responders," in *Proc. DySPAN*, 2008, pp. 1–6.

[65] G. Schelle, J. Fifield, and D. Griinwald, "A Software Defined Radio Application Utilizing Modern FPGAs and NoC Interconnects," in *Proc. Field Programmable Logic and Applications (FPL)*, 2007, pp. 177–182.

[66] L. Nagurney, "Software defined radio in the electrical and computer engineering curriculum," in *Frontiers in Education Conference, IEEE*, 2009, pp. 1–6.

[67] Y. Tachwali, M. Chmeiseh, F. Basma, and H. Refai, "A Frequency Agile Implementation for IEEE 802.22 Using Software Defined Radio Platform," in *Proc. IEEE Globecom*, 2008, pp. 1–6.

[68] SDR-Forum, "A structure for software-defined radio security," Tech. Rep. SDRF-03-I-0010, 2003.

[69] Q. Zhang, A. Kokkeler, and G. Smit, "A reconfigurable radio architecture for cognitive radio in emergency networks," in *EuWiT*.

[70] I. Kuon, R. Tessier, and J. Rose, "Fpga architecture: Survey and challenges," *Found. Trends Electron. Des. Autom.*, vol. 2, pp. 135–253, 2008.

[71] S. Brown and J. Rose, "Fpga architectural research: a survey," *IEEE Design & Test of Computers*, vol. 13, pp. 9–15, 2002.

[72] Z. Quan, S. Cui, and A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, 2008.

[73] F. Digham, M. Alouini, and M. Sinon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. Commun.*, vol. 55, pp. 21–24, 2007.

[74] H. Kim and K. Shin, "In-band Spectrum Sensing in Cognitive Radio Networks: Energy Detection or Feature Detection?" in *Proc. MobiCom*, 2008, pp. 14–19.

[75] S. Gong, W. Liu, W. Yuan, W. Cheng, and S. Wang, "Threshold-Learning in Local Spectrum Sensing of Cognitive Radio," in *Proc. VTC*, 2009, pp. 1–6.

[76] C. Clancy, J. Hecker, and E. Stuntebeck, "Applications of machine learning to cognitive radio networks," *IEEE Wireless Commun.*, vol. 14, 2007.

[77] "Gnu radio, http://www.gnu.org/software/gnuradio."

[78] T. Aysal, S. Kandeepan, and R. Piesewicz, "Cooperative Spectrum Sensing with Noisy Hard Decision Transmissions," in *Proc. ICC*, 2009, pp. 1–5.

[79] Y. Chen, "Collaborative spectrum sensing in the presence of secondary user interferences for lognormal shadowing," *Wireless Communications and Mobile Computing*, 2010.

[80] C. da Silva, B. Choi, and K. Kim, "Distributed Spectrum Sensing for Cognitive Radio Systems," in *Proc. Information Theory and Applications Workshop*, 2007, pp. 120–123.

[81] J. Meng, W. Yin, H. Li, E. Houssain, and Z. Han, "Collaborative spectrum sensing from sparse observations using matrix completion for cognitive radio networks," in *Proc. ICASSP*, 2010, pp. 3114–3117.

[82] B. Shen, K. Kwak, and Z. Bai, "Optimal Linear Soft Fusion Schemes for Cooperative Sensing in Cognitive Radio Networks," in *Proc. Globecom*, 2009, pp. 1–6.

[83] S. Zarrin and T. Lim, "Cooperative Quickest Spectrum Sensing in Cognitive Radios with Unknown Parameters," in *Proc. Globecom*, 2009, pp. 1–6.

[84] W. Zhang, R. Mallik, and K. Letaief, "Cooperative Spectrum Sensing Optimization in Cognitive Radio Networks," in *Proc. ICC*, 2008, pp. 3411–3415.

[85] Y. Zheng, X. Xianzhong, and L. Yang, "Cooperative spectrum sensing based on snr comparison in fusion center for cognitive radio," in *Proc. ICACC*, 2009, pp. 212–216.

[86] Z. Tian, E. Blasch, W. Li, G. Chen, and X. Li, "Performance evaluation of distributed compressed wideband sensing for cognitive radio networks," in *Proc. ISIF*, 2008, pp. 1–8.

[87] J. Fitton, "Security considerations for software defined radios," in *Proc. SDR '02 Technical Conference and Product Exposition*, 2002, pp. 1–7.

[88] C. Li, A. Raghunathan, and N. Jha, "An architecture for secure software defined radio," in *Proc. Date '09*, 2009, pp. 448–453.

[89] S. Xiao, J. Park, and Y. Ye, "Tamper resistance for software defined radio software," in *Proc. COMPSAC*, 2009, pp. 383–391.

[90] E. Noon and H. Li, "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system," in *VTC*, 2010, pp. 1–5.

[91] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," in *Globecom*, 2009, pp. 1–6.

[92] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *DySPAN*, 2010, pp. 1–12.

[93] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[94] C. Murphy, "Combining belief functions when evidence conflicts," *Decision Support Systems*, vol. 29, pp. 1–9, 2000.

[95] "The tcp/ip protocol stack, http://en.wikipedia.org/wiki/TCP/IP_model."

[96] C. Cormio and K. Chowdhury, "A survey on mac protocols for cognitive radio networks," *Elsevier Ad Hoc Networks*, vol. 7, pp. 1325–1329, 2009.

[97] C. Cordeiro and K. Challapali, "C-mac: A cognitive mac protocol for multichannel wireless networks," in *Proc. IEEE DySPAN*, 2007, pp. 147–157.

[98] B. Hamdaoui and K. Shin, "Os-mac: an efficient mac protocol for spectrum-agile wireless networks," *IEEE Trans. Mobile Computing*, vol. 7, pp. 915–930, 2008.

[99] J. Jia, Q. Zhang, and X. Shen, "Hc-mac: a hardware-constrained cognitive mac for efficient spectrum management," *IEEE J. Sel. Areas Commun.* , vol. 26, pp. 106–117, 2008.

[100] L. Ma, X. Han, and C. Shen, "Dynamic open spectrum sharing for wireless ad hoc networks," in *Proc. IEEE DySPAN*, 2005, pp. 203–213.

[101] L. Ma, C. Shen, and B. Ryu, "Single-radio adaptive channel algorithm for spectrum agile wireless ad hoc networks," in *Proc. IEEE DySPAN*, 2007, pp. 547–558.

[102] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive mac for opportunistic spectrum access in ad hoc networks: a pomdp framework," *IEEE J. Sel. Areas Commun.* , vol. 25, pp. 589–600, 2007.

[103] S. Jha, M. Rashid, V. Bhargava, and C. Despins, "Omc-mac: An opportunistic multichannel mac for cognitive radio networks," in *Proc. VTC*, 2009, pp. 1–5.

[104] R. Jain, D. Chiu, and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," Tech. Rep. TR-301, 1984.

[105] M. Cakiroglou and T. Ozcerit, "Jamming detection mechanisms for wireless sensor networks," in *Proc. 3rd Int. Conference on Scalable Information Systems*, 2008.

[106] A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, "MOJO: a distributed physical layer anomaly detection system for 802.11 WLANs," in *ACM MobiSys*, 2006.

[107] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM MobiHoc*, May 2005.

[108] M. Thamilarasu, S. Mishra, and R. Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad hoc networks," in *Proc. Milcom 2006*, October 2006, pp. 1–7.

[109] "The ieee 802.16 working group on broadband wireless access standards, http://www.ieee802.org/16/."

[110] K. Bian and J. Park, "Security vulnerabilities in ieee 802.22," in *Proc. WICON*, 2008, pp. 1–9.

[111] W. Wang, Y. Sun, H. Li, and Z. Han, "Cross-layer attack and defense in cognitive radio networks," in *Globecom*, 2010, pp. 1–6.

[112] A. Toledo and X. Wang, "Robust detection of selfish mishbehavior in wireless networks," *IEEE J. Sel. Areas Commun.* , vol. 25, pp. 1124–1134, 2007.

[113] A. Cardenas, "Evaluation of detection algorithms for mac layer misbehavior: Theory and experiments," *IEEE/ACM Trans. Netw.* , vol. 17, pp. 605–617, 2009.

[114] V. Giri and N. Jaggi, "Mac layer misbehavior effectiveness and collective aggressive reaction approach," in *IEEE Sarnoff Symposium*, 2010, pp. 1–5.

[115] A. Brawerman, D. Blough, and B. Bing, "Securing the download of radio configuration files for software defined radio devices," in *MobiWac*, 2004, pp. 98–105.

[116] H. Uchikawa, K. Umebayashi, and R. Kohno, "Secure download system based on software defined radio composed of fpgas," in *PIMRC*, 2002, pp. 437–441.

[117] X. Li, J. Chen, and F. Ng, "Secure transmission power of cognitive radios for dynamic spectrum access applications," in *Proc. CISS*, 2008, pp. 213–218.

[118] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. Inf. Theory*, vol. 53, pp. 471–487, 2007.

[119] "Vmware server, http://www.vmware.com/products/server."

[120] "Virtualization for embedded systems, http://wiki.ok-labs.com."

[121] "Spec cpu 2006, http://www.spec.org/cpu2006."

[122] R. Cole and J. Rosenbluth, "Voice over ip performance monitoring," in *Proc. ACM SIGCOMM*, 2001, pp. 9–24.

[123] J. Campbell, W. Campbell, D. Jones, S. Lewandowski, D. Reynolds, and C. Weinstein, "Biometrically enhanced software-defined radios," in *Proc. Software Defined Radio Technical Conference*, 2003, pp. 1–6.

[124] L. Michael and M. Mihaljevic, "A proposal of architectural elements for implementing secure software download service in software defined radio," in *PIMRC*.

[125] ——, "Security issues for software defined radio: Design of a secure download system," *IEICE Trans. Commun.*, vol. E85–B, pp. 2588–2600, 2002.

[126] ——, "A framework for secure download for software-defined radio," *IEEE Commun. Mag.*, vol. 40, pp. 88–96, 2002.

[127] A. Brawerman and J. Copeland, "An anti-cloning framework for software defined radio mobile devices," in *ICC*, 2005, pp. 3434–3438.

[128] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Gódor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys and Tutorials*, pp. 1–25, 2011.

[129] "The wimax forum, http://www.wimaxforum.org."

Alexandros G. Fragkiadakis is a Research Associate in the Institute of Computer Science of the Foundation for Research and Technology, Hellas (FORTH-ICS). Dr Fragkiadakis received his PhD in computer networks from the Department of Electronic and Electrical Engineering of Loughborough University in UK. He has also received an MSc in Digital Communications Systems, awarded with distinction, from the same University. Alexandros obtained his Diploma degree in Electronic Engineering from the Technological Educational Institute of Piraeus, Greece. He has worked as a Research Associate within the High Speed Networks Group of the Department of Electronic and Electrical Engineering in Loughborough University. Within FORTH-ICS he has been involved in several projects in the area of wireless communications and networking. His research interests include wireless networks, intrusion detection and security in wireless networks, re-programmable devices, open source architectures, cognitive radio networks, wireless sensor networks.

Elias Z. Tragos is a Research Associate in the Telecommunications and Networks Laboratory (TNL) of the Institute of Computer Science of the Foundation for Research and Technology, Hellas (FORTH-ICS). Dr. Tragos received his diploma in Electrical and Computer Engineering, his MBA in Technoeconomics and his PhD from the School of Electrical and Computer Engineering of the National Technical University of Athens, Greece. He has been actively involved in the WINNER and WINNER II and EU-MESH projects, in the WWI Cross Issues workgroups of System Architecture, System Interfaces and Validation and in many national Greek projects. His research interests are in the area of mobile and wireless networks, mesh and ad-hoc networks, Radio Resource Management, mobility and policy based management, P2P networks and cognitive networks. He is a member of the Technical Chamber of Greece.

Ioannis G. Askoxylakis received a Diploma in Physics from the Physics Department of University of Crete, Greece, in 1998 and a Master of Science in Communication Engineering from the Department of Electrical Engineering and Information Technology of Technical University of Munich, Germany, in 2000. In August 2002 he joined the Telecommunications and Networks Laboratory of FORTH-ICS as a Research Scientist. Within FORTH-ICS he participates in the two Horizontal Programmes of the Institute: the Information Security Programme and the Ambient Intelligence Programme. Since 2009 he coordinates FORTHcert, the Computer Emergency Response Team of the FORTH. He is a member of the Permanent Stakeholders Group of ENISA and member of Future Internet Forum of the European Commission.