Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead

Gianmarco Baldini, *Member, IEEE,* Taj Sturman, *Member, IEEE,* Abdur Rahim Biswas, *Member, IEEE,* Ruediger Leschhorn, *Member, IEEE,* Györzö Gódor, *Member, IEEE,* and Michael Street

***Abstract*—Software Defined Radio (SDR) and Cognitive Radio (CR) are promising technologies, which can be used to alleviate the spectrum shortage problem or the barriers to communication interoperability in various application domains.**

The successful deployment of SDR and CR technologies will depend on the design and implementation of essential security mechanisms to ensure the robustness of networks and terminals against security attacks. SDR and CR may introduce entirely new classes of security threats and challenges including download of malicious software, licensed user emulation and selfish misbehaviors. An attacker could disrupt the basic functions of a CR network, cause harmful interference to licensed users or deny communication to other CR nodes.

The research activity in this area has started only recently and many challenges are still to be resolved. This paper presents a survey of security aspects in SDR and CR. We identify the requirements for the deployment of SDR and CR, the main security threats and challenges and the related protection techniques. This paper provides an overview of the SDR and CR certification process and how it is related to the security aspects. Finally, this paper summarizes the most critical challenges in the context of the future evolution of SDR/CR technologies.

***Index Terms*—Cognitive Radio, Software Defined Radio, Security, Dynamic Spectrum Allocation, Denial of Service, Information Assurance.**

I. Introduction

IN THE PAST decade, Software Defined Radio (SDR) and Cognitive Radio (CR) technology has revolutionized our view of opportunities in wireless communications to a great extent. The key motivation behind this technology is to increase spectral utilization and to optimize the use of radio resources. As SDR and CR are clearly emerging as a strong technological opportunity, research and development is being promoted rapidly throughout the wireless industry and in the academic research arena. Correspondingly, the standardization, regulation and certification activities are also being initiated in many parts of the world including IEEE 802.22, Wireless Innovation Forum and ETSI. However, the security issues on SDR and CR is still under research especially for commercially viable prototypes and future products and its implications on standardization.

SDR technology implements radio functionalities like modulation/demodulation, signal generation, signal processing and signal coding in software instead of hardware as in conventional radio systems. The software implementation provides a higher degree of flexibility and reconfigurability and many benefits including the capability to change the channel assignments, to change the provided communication services or modify the transmission parameters or communication protocols. SDR is also considered a technology enabler for CR, which are "intelligent" radios, which can learn from the environment and adapt their transmission/reception frequencies and parameters to improve spectrum utilization and communication efficiency. SDR and CR technologies are fundamental blocks to provide a more flexible approach to spectrum management in comparison to the conventional approach where radio frequency spectrum bands are statically allocated by spectrum regulators. This flexible approach, known as Dynamic Spectrum Access (DSA) or Dynamic Spectrum Management (DSM), is considered a potential solution for the "spectrum shortage" problem. In the rest of the paper, the term DSA will be used. A more detailed description of SDR and CR concepts is provided in section II.

One of the major challenges for the wide deployment of SDR and CR technology is to provide an adequate level of security. It is well known that security is an important element in wireless communications. While SDR and CR based systems should guarantee the same level of security of conventional wireless communication systems, they may also present new vulnerabilities or security threats.

As a general rule, communication systems based on SDR and CR technology must validate communication security requirements like Data Confidentiality and Privacy, Availability, Registration, Authentication and Authorization. This is a consequence of the general conformance to standards and regulations already defined for the wireless communication systems, with which SDR and CR devices must interoperate. For example, if SDR and CR devices are used in the public

Manuscript received 16 July 2010; revised 29 December 2010.

G. Baldini is with the Joint Research Centre of the European Commission, Ispra, Italy (e-mail: gianmarco.baldini@jrc.ec.europa.eu).

T. Sturman is with EADS Astrium, Portsmouth, UK (e-mail: taj.sturman@astrium.eads.net).

A. R. Biswas is with CREATE-NET, Trento, Italy (e-mail: abdur.rahim@create-net.org).

R. Leschhorn is with Rohde & Schwarz, Munich, Germany (e-mail: Ruediger.Leschhorn@rohde-schwarz.com).

G. Gódor is with the Budapest University of Technology and Economics (BUTE), Budapest, Hungary (e-mail: godorgy@hit.bme.hu).

M. Street is with the NATO Agency, Brussels, Belgium (e-mail: Michael.Street@nc3a.nato.int).

Digital Object Identifier 10.1109/SURV.2011.032511.00097

safety domain, they should satisfy the government approved security requirements defined by the TETRA or APCO 25 standards.

SDR and CR concepts may provide new powerful capabilities but they may also be vulnerable to new types of security attacks, beyond the ones already defined for conventional networks.

The principal accessibility of a SDR's computer code for dynamic (de)installation and (un)loading of radio applications can introduce new security vulnerabilities in comparison to conventional radio systems, where the radio application is embedded in the design of the components.

The promise of CR to realize a flexible spectrum management framework (e.g. DSA) by implementing sophisticated algorithms for spectrum awareness and improved spectrum utilization should be evaluated for security and reliability. Security attacks could be implemented against cognitive elements of the network by providing wrong information on the radio environment or by influencing the cognitive radio mechanism itself.

The purpose of this paper is present a survey of security aspects of SDR and CR technologies, the most relevant security threats, the related protection techniques and countermeasures. Most of the threats, requirements and protection techniques apply on high level to all three domains (commercial, public safety and military). Military specific considerations are basically beyond the scope of this paper.

The rest of the paper is organized as follows. Section II describes the general concepts of SDR and CR. Section III identifies and describes the security requirements. Section IV describes the threats for SDR and CR technologies. The section also describes the methodology used to classify the threats and evaluate the impact in relation to the security requirements. Section V describes the countermeasures and protection techniques in SDR and CR. Section VI describes how security threats are addressed in current SDR/CR standards. Security certification of SDR/CR systems and devices is presented in Section VII. Section VIII focuses on the "way ahead" in this research area: it summarizes the outstanding challenges and identifies actions in the context of the future evolution of SDR/CR technology. Finally section IX concludes the paper.

II. Software Defined Radio and Cognitive Radio

The concept of SDR has evolved from the seminal work of Joseph Mitola in [1]. Over this period a number of references have provided their definition of SDR, which has given rise to various interpretations of what SDR actually is and what is not. A key reason is that SDR is an all embracing term, which may be applied to a wide range of radio platforms and concepts. In ETSI [2], SDR is defined as "radio in which the radio frequency (RF) operating parameters including, but not limited to, frequency range, modulation type, or output power can be set or altered by software, and/or the technique by which this is achieved".

An alternative definition is provided by the SDR Forum, now named Wireless Innovation Forum [3], which has developed a definition of SDR in cooperation with IEEE working group P1900.1:

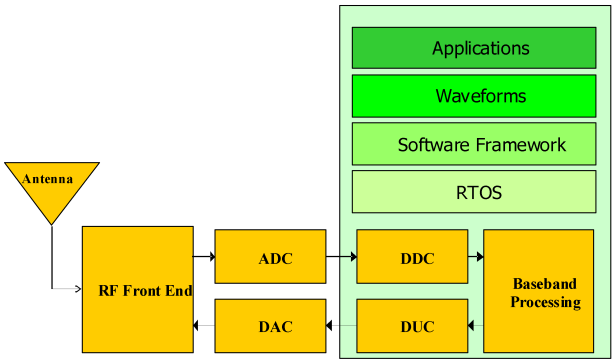

Fig. 1. Example of Software Defined Radio architecture; ADC (analog to digital conversion, DAC (digital to analog conversion), DDC (digital down conversion, DUC (digital up conversion

"Radio in which some or all of the physical layer functions are software defined".

The Forum explains: "An SDR defines a collection of hardware and software technologies where some or all of the radio's operating functions (also referred to as physical layer processing) are implemented through modifiable software or firmware operating on programmable processing technologies. These devices include field programmable gate array (FPGA), digital signal processors (DSP), general purpose processor (GPP), programmable system on chip (SoC) or other application specific programmable processors. The use of these technologies allows new wireless features and capabilities to be added to existing radio systems without requiring new hardware".

Figure 1 provides a potential architecture of a SDR and its main elements starting from the *Real Time Operating System (RTOS)*. The *Software Framework* provides basic functions and libraries to support the waveforms and their portability including the middleware. An example of software framework is the combination of Software Communications Architecture (SCA) and CORBA middleware described in [4]. The *waveform* represents the software implementation of a communication service (e.g. UMTS). Finally, *applications* can be defined to support a specific operational or business context.

In ETSI [2], a CR is defined as "radio, which has the following capabilities: to obtain the knowledge of radio operational environment and established policies and to monitor usage patterns and users' needs; to dynamically and autonomously adjust its operational parameters and protocols".

The design and deployment of CR and DSA have been investigated in a number of papers and research studies starting from the paper of Joseph Mitola [5].

It is usually recognized that CRs should provide the following functions:

1) determine which portions of the spectrum are available and detect the presence of licensed users when a user operates in a licensed band (spectrum sensing),

2) select the best available channel (spectrum management) for communication,
3) coordinate access to this channel with other users (spectrum sharing), and
4) vacate the channel when a licensed user is detected (spectrum mobility).

These functions are dependent on each other as described in Figure 2. The figure describes also the relationships among the functions. For example: spectrum mobility can alert the spectrum sensing function on detected changes in the spectrum environment. Acting on the alert, the spectrum sensing function can collect again the knowledge of the spectrum environment and provide it to the spectrum management function to re-plan the allocation of spectrum bands.

The disruption of spectrum sensing has an impact on the other functions because they will not have the needed information to perform effectively. Spectrum management requires the knowledge of the spectrum environment acquired by spectrum sensing to select the best available channel. Spectrum sharing needs the information on the bands selected by spectrum management function in each node. Spectrum mobility needs information on spectrum environment changes from spectrum sensing and the current allocation of spectrum bands from spectrum management and spectrum sharing. CR networks are composed by many nodes, with different capabilities, which interact on the basis of defined protocols and policies. To implement and deploy DSA, CR nodes do not operate in isolation but they are part of wider CR networks, which must provide a higher set of capabilities, which include context awareness and resource management. Context awareness means that a node or a network should be aware of the operational context, existing policies and regulations, network and spectrum awareness and user requirements in terms of requested traffic capacity, quality of service (QoS), resilience and security. Resource management means that CR nodes must cooperate to allocate the available network or spectrum resources, not only internally but also externally to other conventional networks. Each of these capabilities can be disrupted by intentional or unintentional threats. For example: a malicious attacker can implement a security attack against the resource management capability to allocate network or spectrum resources to itself or simply to provoke a Denial of Service (DoS) activity.

A survey of CR networks and the related architectures is presented in [6], where the authors describe the various CR techniques and architectures to implement DSA and CR networks.

The two most common approaches are *collaborative* and *uncooperative*:

1) In the *collaborative* approach, the cognitive functions are based on the coordination of the CR nodes, which exchange information to optimize the spectrum utilization and to improve the efficiency of the network.
2) In the *uncooperative* approach, each CR node implements the cognitive functions on its own.

The collaborative approach is usually considered more efficient, faster to converge to shared spectrum resources allocation and more reliable than the uncooperative approach but it requires common channels to exchange information. The common channel is often called Cognitive Control Channel (CCC) [7] and it is responsible for distributing the cognitive messages in the CR network.

In turn, the collaborative approach can be *centralized* or *distributed*. In a centralized solution, a central node, e.g. a base station (BS), controls the allocation of the spectrum resources or collects the spectrum sensing information. In the distributed solution, the CR nodes must agree on a common spectrum allocation through decision algorithms or voting systems. A centralized solution may be more efficient but the central node can represent a single point of failure. A comparison between the centralized and distributed approaches for spectrum management is presented in [8].

Furthermore, a centralized solution may imply the presence of an existing infrastructure or pre-existing contracts to identify the centralized node.

Each of the proposed CR architectures has different levels of vulnerability against specific security threats.

III. Security Requirements

The National Security Agency (NSA) defines Information Assurance IA [9] as the set of "measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation".

Note that security requirements are not only limited to the protection of the data stored or transmitted by the network but also that the communication system is able to guarantee the services defined by the operational requirements.

As described in [10], the definition of the security requirements may be derived considering the concepts of stakeholders, asset, threat and risk.

The *stakeholders* can be users of the communications systems, public and government authorities or the network providers. *Assets* include the components of the network, the information stored or transmitted and the services provided by the network.

A *security threat* is defined as a potential violation of security. Examples of security threats are loss or disclosure of information or modification/destruction of assets. A security threat can be intentional like a deliberate attack or unintentional due to an internal failure or malfunctions.

The *security risk* measures the impact of the realization of a security threat. *Security countermeasures* (protection techniques) strive to eliminate or reduce the security risks.

In this paper, the definition of security requirements is an extension of the network security requirements defined by the International Telecommunications Union (ITU) in [11].

The following security requirements are defined:

1) *Controlled access to resources*: the system should ensure that actors are prevented from gaining access to information or resources that they are not authorized to access.

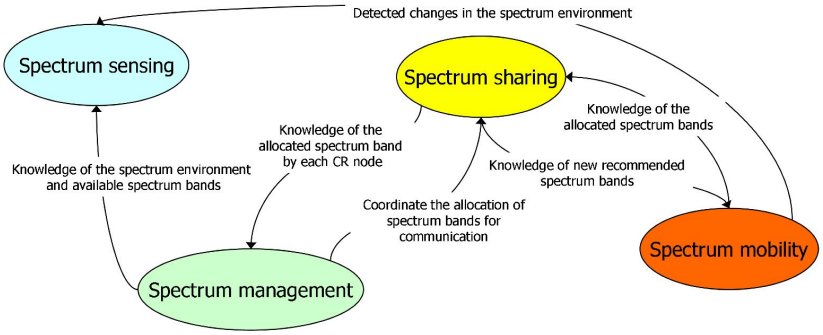

Fig. 2. Dependencies among cognitive radio functions

2) *Robustness*: the system should be able to provide the required communication services as described in specific service level agreements. For example: a service level agreement can specify the required QoS or traffic capacity. This requirement is related to the capability of the system to resist threats, which have the objective to deny one or more system services.
3) *Protection of confidentiality*: the system should provide capabilities to ensure the confidentiality of stored and communicated data.
4) *Protection of system integrity*: the systems should be able to guarantee the integrity of system and its components.
5) *Protection of data integrity*: the system should be able to guarantee the integrity of stored and communicated data.
6) *Compliance to regulatory framework*: the system should be able to guarantee the compliance to the regulations active in the area, where the system operates.
7) *Accountability*: the system should ensure that an entity cannot deny the responsibility for any of its performed actions. In this context, accountability is used as a synonym of Non-Repudiation.
8) *Verification of identities*: a telecommunication network should provide capabilities to establish and verify the claimed identity of any actor in the telecommunication network.

Communication systems based on SDR/CR should provide the capabilities to address security threats, which may undermine the requirements described above.

IV. Software Defined Radio and Cognitive Radio Threats

The purpose of this section is to describe the list of potential threats to SDR and CR. The threats will be classified on the basis of the following criteria:

- Security requirements, which are invalidated by the threat.
- Affected SDR or CR function (e.g., spectrum sensing).
- Whether the threat is intentional or unintentional.

A. Software Defined Radio threats

A major security issue introduced by the SDR is the consequence of its reconfiguration capability, as described in [11]. Theoretically, SDR terminals should be able to download new radio applications or waveforms (e.g., through the air interface or through fixed communication links). Once activated, the radio application will change the radio transmission parameters like frequency, power, and modulation types.

This capability presents two main security issues:

1) Who guarantees that the downloaded profile or software module (e.g., waveform or radio application) comes from a trusted source and can be activated on the SDR device?
2) Who guarantees that the downloaded profile or software module will behave as expected?

SDR BSs will be usually connected through fixed or highly secured wireless connections. In this sense, the security threats and mechanisms are very similar to conventional wireless systems, and the standard secure software download mechanism already defined in cellular networks could be applicable to networks based on SDR technology. If the software is downloaded over the air, there is a possibility that an attacker could illegally obtain the software, alter it, or change it with a malicious copy.

An attacker can download a malicious software module or profile to the SDR terminals in the coverage area of the network. In this sense, SDR can be vulnerable to the same type of attacks of personal computers connected to the Internet, including virus, worms, and other malware. The significant difference between a personal computer and SDR is that an SDR terminal, which has been taken over, can disrupt a wireless network or other wireless networks in the area by creating harmful interference. Because SDR terminals can be designed to transmit in a wide range of frequencies, the potential for network disruption is very high.

We identify the following functionalities in SDR, which can be affected by security threats:

1) *Application management*, which includes waveform download and activation.
2) *Resource management* of computing and processing internal resources of the SDR.
3) *Data management* to store and retrieve the configuration data used by the waveforms and the operating environment.
4) *Internal data transport* for the distribution of data among the various modules of the SDR.

In our model, these functionalities are considered *assets* impacted by security threats. Each of the threats can be directed against one or more SDR components described in Figure 1, including the RTOS, the software framework, and the waveforms.

A specific type of *asset* is the data in the SDR. We can identify different types of data:

- *user data*, which represents the data exchanged and stored in the SDR by the network user.
- *configuration data*, which is used by the RTOS and *Software Framework*. Configuration data include control data and parameters to manage the SDR resources.
- *waveform code*, which includes the parameters needed by the specific waveform. For example, the reception and transmission parameters.

Table I presents the list of security threats. The ID is used to reference the security threats in the rest of the paper.

The description of the threats is as follows:

1) *Insertion of malicious software*. This threat identifies the insertion of malicious software on an SDR. This threat is similar to mobile malware in mobile applications.
2) *Alteration or destruction of the configuration data*. This threat identifies the alteration or destruction of configuration data, which is needed by the SDR to perform its functions. Configuration data can be corrupted or removed from the SDR platform.
3) *Artificial consumption of resources*. This threat identifies the abnormal increase in processing or memory resources of the SDR platform to cause DoS. This threat can be induced by various causes, including the consequence of threat 1 or 2 or a physical failure.
4) *Alteration or destruction of waveform code*. This threat identifies the alteration or destruction of the waveform code, which is needed to support a radio access technology (RAT) or air interface. This threat may affect one or more waveforms but not the SDR itself.
5) *Alteration or destruction of real-time operating system*. This threat identifies the alteration or destruction of components or the RTOS. This threat may affect all the waveforms and the functions of the SDR itself.
6) *Alteration or destruction of the software framework*. This threat identifies the alteration or destruction of elements of the software framework and middleware, which support the waveforms and applications. This threat may affect all the waveforms and the functions of the SDR itself.
7) *Alteration or destruction of user data*. This threat identifies the alteration or destruction of user data, like customized profiles of the waveforms and applications. Without user data, the behavior of the SDR can be set back to the default status.
8) *Software failure*. This threat identifies a generic software failure in the any of the components composing the real-time operating system, the software framework, waveforms, or applications.
9) *Hardware failure*. This threat identifies a generic hardware failure in the SDR HW platform. For example, a failure in the amplifiers, the filters, or the FPGA.
10) *Extraction of configuration data*. This is an eavesdropping threat, where an attacker collects configuration data, which can be used in subsequent attacks.
11) *Extraction of waveform data*. This is an eavesdropping threat, where an attacker collects waveform data, which can be used in subsequent attacks.
12) *Extraction of user data*. This is an eavesdropping threat, where an attacker collects user data, which can be used in subsequent attacks.
13) *Masquerading as authorized software waveform*. This threat identifies the download and activation of a malicious software waveform on the SDR platform. This is one of the most serious attacks as the download of waveforms is considered an important function of the SDR. A malicious waveform can disrupt the SDR network or affect conventional wireless networks through harmful interference.
14) *Unauthorized use of Software Defined Radio services*. This threat identifies a security breach, where a waveform or applications can access or use services of the SDR platform for which it does not have the proper access level. For example, a malicious waveform could access specific cryptographic services to decode incoming secure transmissions.
15) *Data repudiation*. This threat identifies the possibility of repudiating the access or provision of data and services.

We can classify these threats in two broad categories:

1) Threats which are common both to SDR technology and to conventional communication radio systems.
2) Threats which are specific to SDR technology.

1) Common threats:

Threats T(8) and T(9) are present in conventional wireless communication systems, and conventional high assurance solutions can be adopted for SDR technology as well, with the difference that many critical components could be implemented in software instead of hardware. Reference [13] presents reliability and availability requirements and solutions for SDR technology for space telecommunications. Reference [14] presents a system threat analysis for SDR to improve its high assurance.

Threat T(10) can be implemented by having access to the SDR platform and extracting configuration data and parameters. This type of threat is not different from privacy violation attacks against a generic mobile computing platform, as described in [15]. An attacker can use the obtained information to increase the effectiveness of attacks for other security threats.

Threat T(11) can be implemented by extracting data in the SDR platform itself or during the SDR software download. The first case requires access to the platform functions and data, and it is not different from extracting data from a computing or storage device and it is extensively investigated in data security research. Reference [16] provides a comprehensive view of privacy engineering and the related design solutions. Extraction of the waveform data during software download requires advanced technical capabilities by the attacker to intercept the signal in the space, demodulate it, and extract the

TABLE I
SOFTWARE DEFINED RADIO SECURITY THREATS

Threat ID	Threat Description	Security Requirement	Affected Functionality
T(1)	Insertion of malicious software	Protection of system integrity	Application management
T(2)	Alteration or destruction of the configuration data	Protection of data integrity	Application management, Resource management
T(3)	Artificial consumption of resources	Robustness	Resource management
T(4)	Alteration or destruction of waveform code	Protection of system integrity	Application management
T(5)	Alteration or destruction of real-time operating system software	Protection of system integrity	Application management
T(6)	Alteration or destruction of the software framework	Protection of system integrity	Application management
T(7)	Alteration or destruction of user data	Protection of data integrity	Internal data transport, Data management
T(8)	Software failure	Protection of system integrity, Robustness	All functionalities
T(9)	Hardware failure	Protection of system integrity, Robustness	All functionalities
T(10)	Extraction of configuration data	Protection of confidentiality	Internal data transport, Data management
T(11)	Extraction of waveform data	Protection of confidentiality	Internal data transport, Data management
T(12)	Extraction of user data	Protection of data integrity	Data management
T(13)	Masquerading as authorized software waveform	Protection of system integrity, Verification of identities, Controlled access to resources, Accountability	Application management
T(14)	Unauthorized use of software defined radio services	Verification of identities, Controlled access to resources, Protection of system integrity	All functionalities
T(15)	Data repudiation	Verification of identities, Protection of data integrity	Internal data transport, Data management

information. This task is difficult but not impossible depending on the security countermeasures adopted for secure software download.

Loss of data (threat T(12)) is a common threat in communication systems. The attacker should have access to internal data management function of the SDR platform to implement this threat. The impact of this threat is serious as the SDR platform may not function and provide the needed services to the rest of the network.

Breach of data repudiation, T(15), can impact any exchange of information on the SDR platform. The most serious risk is the verification and trust of signatures used to mitigate the other security threats. The extensive research activity for data repudiation in mobile computing (see [17]) could be adapted to the SDR technology.

2) *Specific SDR threats:*

Most of these threats have already been identified in the literature. Reference [18] describes the security threats to a GNU radio platform, where all downloaded software modules share a single address space. Security threats to generic software defined radios are also presented. In [19] is presented a recent overview of SDR security issues and challenges. Protection against unauthorized software activation is considered a major challenge.

Security threat T(1) for the insertion of malicious software downloaded from an external source is addressed in [20] and [21]. Both the papers address a security attack where malicious software is downloaded or where a software module is illegally modified before the download.

Reference [22] identifies T(6), T(8), and T(14) as the main security threats to SDR. Experience from the computing world (e.g., PC) has shown that it is very difficult to detect security holes or Trojan horses (e.g., unauthorized software) in the product-testing phase. Protection techniques and countermeasures are also described.

Reference [23] describes the unauthorized use of services of another SDR device, which is commonly described in conventional wireless communications as "device cloning." In this paper, "device cloning" is identified as security threat T(13) if the waveform is affected or security threat T(14) if SDR services are affected.

Malicious reconfiguration of the SDR (associated with security threats T(2), T(3), T(4), T(5), T(6), T(7), and T(13)) is explored in [24], which describes the increased vulnerability of SDR in comparison to conventional communication systems because even the software implementations of the security module are vulnerable to malicious modifications. Even if an integrity checking mechanism is introduced, it may be modified/blocked by a malicious operating environment (such as a compromised OS or middleware). T(3) is also suggested in [23] in relation to the SDR infection by specific viruses (e.g., Trojan horses).

B. Cognitive Radio threats

Conventional communication systems can only change their transmission parameters and use the radio frequency (RF) spectrum bands in the limits, which have been defined by predefined standards and spectrum regulations. These limits are implemented in their hardware and firmware architecture,

and they cannot be changed at runtime. A CR may instead communicate in a wide range of spectrum bands and may have the capability to change its transmission parameters at runtime in response to changes in the sensed radio spectrum environment, information received from other CR nodes, or networks.

This capability can be used to implement innovative approaches to spectrum management, like DSA described in section II, where the allocation of spectrum bands to communication services can change in time or space. A CR, which has been taken over by an attacker, can break the DSA mechanism by implementing spectrum misusage or selfish behavior. For example, it can transmit in unassigned bands or it can ignore the cognitive messages sent by other elements of the network. DSA can be implemented using various architectures for CR networks. As described in section II, CR network architectures can have many different classifications. While there are common security attacks, each architecture may present specific vulnerabilities.

In literature, a majority of the centralized or distributed approaches assume that the participating nodes are altruistic and make logical decisions to optimize the spectrum resources. Such approaches make the CR network vulnerable to security threats, where malicious CR nodes implement selfish behavior or would like to disrupt the protocols and algorithms defined to converge to optimal spectrum utilization.

It is of crucial importance to identify the various types of security attacks and the related protection measures. Masquerading is a threat frequently cited in research literature. In this threat, a malicious CR node provides false information for the CR functions (e.g., spectrum sensing or spectrum sharing). The malicious CR node can inject false information on the spectrum environment into the other CR nodes with the objective of gaining an unfair advantage or just disrupting the CR network. This type of threat can affect both centralized and distributed CR networks.

The distribution of incorrect or incomplete information on the spectrum environment can also be unintentional. In the case of the hidden node problem, two CR devices may have a different perception of the spectrum because they are located in two different locations and they detect different radio spectrum information (see Figure 5). The hidden node problem is also called the hidden incumbent problem.

An obvious DoS threat is jamming. Jamming can be used to a) hamper or obstruct all the communications in a specific spectrum band or b) disrupt the management channels of the CR networks, which are used to distribute the cognitive messages among the CR nodes. A survey of jamming attacks on wireless networks is presented in [25].

Table 2 identifies the CR threats. As described before, we identify the following CR functions, which can be impacted by a security threat: spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility.

A pictorial description of the main CR threats is presented in Figure 3.

The description of the threats is as follows:

1) *Jamming of the channel used to distribute cognitive messages*. This threat identifies the jamming of a cognitive control channel (CCC) used to distribute cognitive messages in the CR network. Jamming can be executed against an out-of-band CCC or an in-band CCC if the frequency of the channel is known.
2) *Malicious alteration of cognitive messages*. This threat identifies the alteration of cognitive messages exchanged in the CR network.
3) *Masquerading of a primary user*. This threat identifies the malicious masquerading of a primary user like a digital TV broadcaster. The malicious attacker may mimic the primary user characteristics in a specific frequency band (e.g., white space band), so that the legitimate secondary users erroneously identify the attacker as an incumbent and they avoid using that frequency band. This can be a selfish attack, because the attackers may then use the frequency bands or just a DoS attack to deny spectrum resources to other secondary CR users. An example of the masquerading of a primary user is provided in Figure 4. A malicious CR terminal transmits a signal very similar to the primary user. Other CR terminals detect the presence of an additional primary user, and they avoid using the spectrum bands.
4) *Malicious alteration of a cognitive radio node*. This threat identifies the alteration of the behavior of a CR node, which can be used to support other threats like harmful wireless interference to primary or secondary users or disruption of the CR network.
5) *Internal failure of cognitive radio node*. This threat identifies the failure of a CR node, which can have different causes: memory fault, physical failure, or others. This threat may have various impacts, depending on the type of failure. For example, the CR node can transmit in the wrong frequency band or not participate in the CR functions with other CR nodes.
6) *Masquerading of a cognitive radio node*. This threat identifies the masquerading of a CR node while collaborating with other CR nodes for CR functions: spectrum sensing, spectrum sharing, spectrum management, and spectrum mobility. For example, a malicious device can send wrong spectrum sensing information to other CR nodes.
7) *Hidden node problem*. This threat identifies the case in which a CR node is in the protection region of an incumbent node (i.e., the coverage area of a digital TV broadcaster) but fails to detect the existence of the incumbent. An example of the hidden node problem is shown in Figure 5. A CR terminal does not sense the presence of a Primary User BS because of an obstacle (e.g., a mountain). As a consequence, it transmits in the same frequency bands of the primary user, causing harmful interference. Depending on their position, other CR terminals sense a different spectrum environment, and they can provide additional information to mitigate the threat.
8) *Unauthorized use of spectrum bands for selfish use*. This threat identifies the case where a malicious node or CR network uses spectrum bands for which is it not authorized or licensed, to gain more traffic capacity or bandwidth.
9) *Unauthorized use of spectrum bands for DoS to primary*

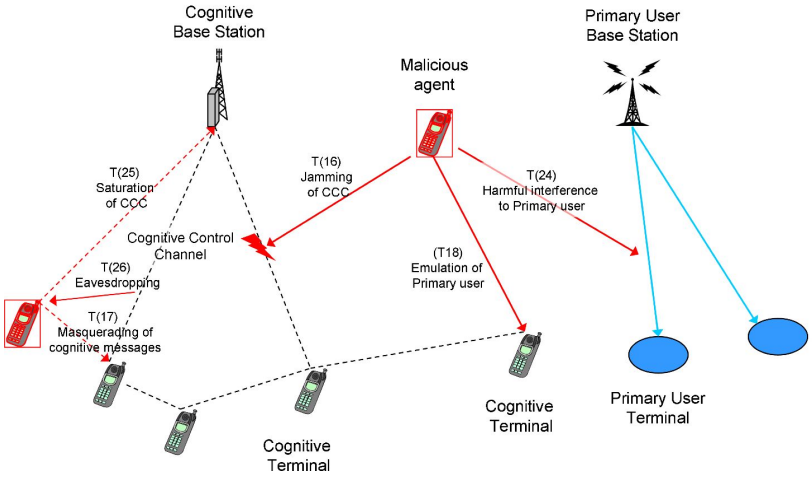

Fig. 3. Cognitive Radio Threats

users. This threat identifies the case where a malicious node or CR network emits power in unauthorized spectrum bands to cause DoS to primary users.

10) *Saturation of the cognitive control channel*. This threat identifies a DoS attack against the cognitive control channel (CCC) by saturation: a large number of cognitive messages are sent to the CCC to deny its service to the CR network. Note that specific designs of the CCC may prevent this type of attack.
11) *Eavesdropping of cognitive messages*. This threat identifies the eavesdropping of cognitive messages by a malicious attacker, who can then use this information for subsequent attacks.
12) *Disruption to the MAC, network layer, or cognitive engine of the cognitive radio network*. This threat includes attacks against the higher functions of the CR network, including the MAC, network layer, and cognitive engine.

We can classify these threats in two broad categories:

1) Threats that are common both to CR technology and to conventional communication radio systems.
2) Threats that are specific to CR technology.

1) Common threats:

Common threats are limited to T(16) and T(20). Some threats (e.g., eavesdropping, masquerading, and saturation) are also possible in conventional wireless communication systems, but their implementation and impact are quite specific for a CR network and they are classified as the second category (i.e., specific to CR technology).

Threat T(16) is investigated in [31], which describes how jamming attack across multiple channels can be implemented by using a single malicious CR node.

A description of the jamming threat is also proposed in [32], which describes in detail the various types of jamming attacks and their impact on the CR networks. The paper identifies four goals for a jammer attack: a) the immediate DoS attack on the CR node, b) cause degradation of the CR network, c) learn the behavior of the CR network to implement other threats, and d) herding, where the jamming attack has the purpose to drive the CR node or network to a specific state, where another security threat could be implemented. For example, the jamming attack can push the CR network to select a specific frequency band for the CCC, where another malicious node can implement the eavesdropping of cognitive messages.

Threat T(20) is identified in reference [44] in relation to the spurious emissions related to equipment aging or misconfigurations. This is a common problem in wireless communication equipment, but it may have a serious impact in CR networks, because it may alter the perception (i.e., spectrum sensing) or behavior (e.g., spectrum sharing, spectrum management, and spectrum mobility) of the cognitive engine.

C. Specific cognitive radio threats

Surveys of specific security threats to CR networks are presented in [26], [27], [28], and [29] using different classifications.

Reference [26] provides a comprehensive description of DoS threats and an associated risk analysis method called the "Hammer model framework" to graphically depict the potential risk sequences relevant to the threat. Reference [26] describes in detail threats T(16), T(17), T(18), and T(21) and relates them to the vulnerabilities of the various CR network architectures. The paper describes the risk level posed by the potential attacks in the different CR design paradigms (i.e., collaborative, uncooperative, centralized, and distributed). A similar approach is proposed in this paper, and it is described in section V, where protection techniques are identified. One of the results of the paper is that non-cooperative CR design seems the most vulnerable, while the distributed cooperative seems the most robust.

In [27], threats are classified on the basis of the CR functions. In [28], security threats are classified on the basis of the type of anomalous behavior, like misbehaving, selfishness, cheating, and malicious. Reference [29] delineates the key challenges in providing security in cognitive networks, discusses the current security posture of the emerging IEEE 802.22 CR standard, and identifies the potential vulnerabilities. The paper advocates a multi-disciplinary approach, which

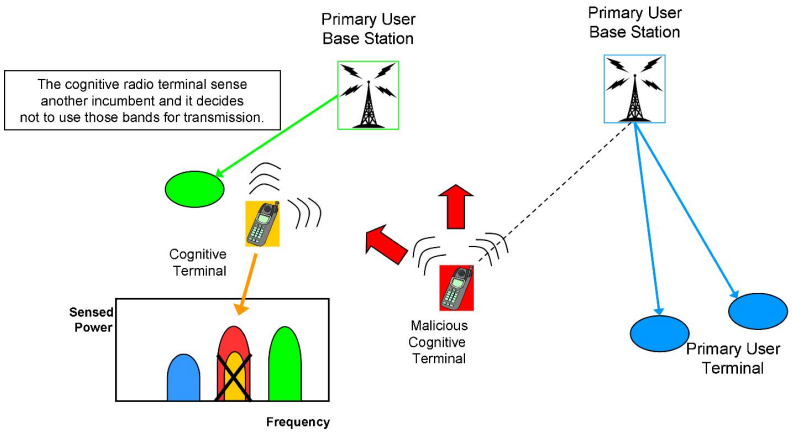

Fig. 4. Masquerading of a primary user

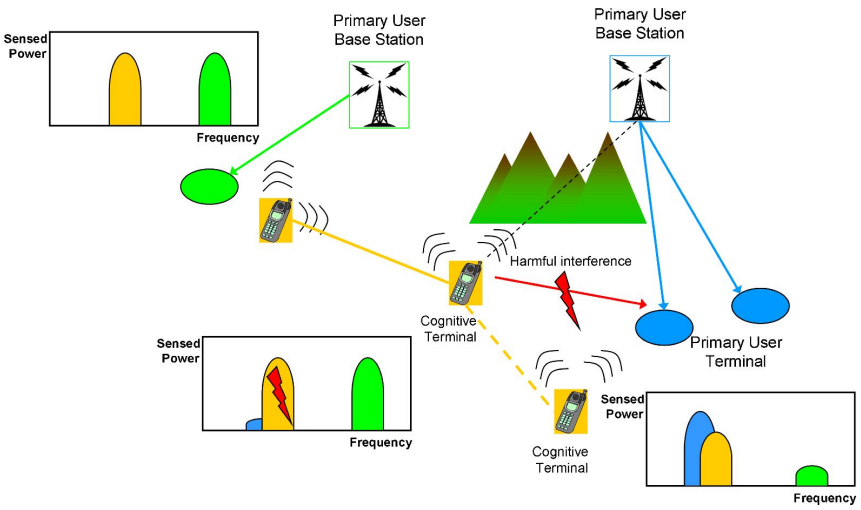

Fig. 5. Hidden Node problem

improves the decision making process of the CR networks to improve their resilience against security threats. Security threats are also associated with the standardization activity of the IEEE 802.22 CR standard. Further details on the security aspects of IEEE 802.22 are described in section VI.

The paper describes the risk level posed by the potential attacks in the different CR design paradigms (collaborative, uncooperative, centralized, and distributed); this approach is proposed in this paper, and it is described in section V where protection techniques are identified.

Reference [30] provides a multidimensional analysis and assessments of DoS CR threats. The threats are assessed against the CR architectures and components. The authors suggest that cooperative network architectures (especially the ones based on a centralized approach) are more resilient than non-cooperative architecture.

Threat T(18) is described in [33], [34], and [35], where a CR node implements a primary user emulation (PUE) attack by transmitting signals whose characteristics emulate those of incumbent signals. Threat T(18) is also investigated in [36], which presents simulation results for attacks based on the manipulation of the feature extraction algorithms and the classifier engines. The identification of the malicious attacker may require sophisticated signal classification algorithms, which are difficult to implement in commercial hand-held terminals.

The PUE attack or threat T(18) is also investigated in [37], which proposes an analytical model to study the feasibility of a PUE. The simulations show that the probability of a successful PUE attack increases with the distance between the primary transmitter and secondary users.

Masquerading attacks and alteration of cognitive messages (threats T(17) and T(21)) in the spectrum sensing function are areas that have received considerable attention by the research community and the related threats are described in [33],[38],[39], and [40].

Threat T(17) is investigated in [41] and [42], where an abnormality detection approach is used to detect malicious secondary user(s), who send false reports in collaborative sensing networks. Threats T(16) and T(25) are addressed in [43]. Reference [44] investigates the security threats and vulnerabilities of the standard IEEE 802.22, which will be the first CR standard to deploy wireless regional area networks (WRANs) using white spaces in the TV frequency spectrum. The classification is slightly different from the one used in this paper, but threats T(16), T(17), T(18), T(19), and T(21) are identified in a similar way.

TABLE II
COGNITIVE RADIO SECURITY THREATS

Threat ID	Threat Description	Security Requirement	Affected functionality
T(16)	Jamming of the channel used to distribute cognitive messages	Robustness, Protection of system integrity	Spectrum sensing, Spectrum sharing
T(17)	Malicious alteration of cognitive messages	Protection of data integrity, Verification of identities	Spectrum sensing, Spectrum sharing
T(18)	Masquerading of a primary user	Verification of identities, Accountability	Spectrum sensing, Spectrum mobility
T(19)	Malicious alteration of a cognitive radio node	Protection of system integrity, Compliance to regulatory framework	Spectrum management, Spectrum sharing, Spectrum mobility
T(20)	Internal failure of cognitive radio node	Protection of system integrity, Robustness	Spectrum sharing, Spectrum mobility
T(21)	Masquerading of a cognitive radio node	Verification of identities, Accountability, Protection of confidentiality, Controlled access to resources	Spectrum sensing, Spectrum sharing, Spectrum management
T(22)	Hidden node problem	Compliance to regulatory framework, Verification of identities	Spectrum sensing, Spectrum sharing, Spectrum mobility
T(23)	Unauthorized use of spectrum bands for selfish use	Compliance to regulatory framework	Spectrum sharing, Spectrum mobility
T(24)	Unauthorized use of spectrum bands for DoS to primary users	Compliance to regulatory framework	Spectrum sharing
T(25)	Saturation of the cognitive control channel	Robustness, Protection of system integrity	Spectrum sensing, Spectrum sharing
T(26)	Eavesdropping of cognitive messages	Protection of confidentiality	Spectrum sensing, Spectrum sharing
T(27)	Disruption to the MAC or the cognitive engine of the Cognitive Radio network.	Verification of identities, Controlled access to resources, Protection of system integrity	Resource management, Data management

Threat T(27) is discussed in [46], which provides a security analysis for CR network MAC protocols. Firstly, the authors investigate how a DoS attack is launched in multi-hop CR network MAC protocols. Then, they explore MAC layer greedy behaviors in CR network.

Threats against the cognitive engine of CR network are described in [100], which defines three classes of threats in this area: sensory manipulation attacks against policy radios, belief manipulation attacks against learning radios, and self-propagating behavior leading to CR viruses. All these types of threats have the objective of manipulating the behavior of a CR system such that it acts either sub-optimally or even maliciously. These types of threats are more sophisticated than basic jamming, as their intention is to disrupt the learning cognitive engine and degrade the performance of the CR network. By repeatedly providing false information, a CR network may decide not to use spectrum bands to the full extent or use a modulation with lower data rates than possible. Reference [100] also describes a propagating attack where a malicious attacker forces a change of state in a CR node, where it is not performing effectively. In turn, the CR node may provide false information to another CR node, propagating the state changes and impacting the overall CR network. The result is effectively a CR virus.

At the current time, threats T(17) and T(18) are considered the main priority by the research community because they directly impact the spectrum sensing function, which is the first phase of the CR cycle as described in section II. Threat T(22) (hidden node) has been extensively investigated in research literature (see [84], [94], and [95]) and various protection techniques have been proposed (e.g., cooperative CR networks). More details on the protection techniques are described in section V.B.

The threats can also be correlated to implement a two-phase attack. For example, an attacker can use security threat T(26) to improve the effectiveness of security threat T(17). First, the attacker eavesdrops on a cognitive message to learn the format and content. Then, the attacker replicates and modifies the cognitive message to transmit false information to disrupt the network or to gain access to spectrum bands (i.e., selfish behavior).

Figure 6 describes how each security threat can contribute to other security threats.

V. SOFTWARE DEFINED RADIO AND COGNITIVE RADIO PROTECTION TECHNIQUES

A. Software Defined Radio protection techniques

As described in section IV, an SDR can be vulnerable to the same type of attacks implemented against conventional software computing platforms by downloading and activating malicious software (threat T(1)), through the external interfaces of the SDR node. By inserting malicious software, an attacker may implement a variety of security threats:

- Alter or destroy configuration data of the SDR node (threat T(2)).
- Implement DoS attacks by overusing computing resources (threat T(3)).
- Alter or destroy other software waveforms (T(4)), the RTOS (T(5)), or the software framework (T(6)), even if this would imply access to specific rights and permissions.
- Masquerade as a software waveform (T(13)).
- Destroy data on the SDR node (T(12)).
- Unauthorized use of SDR radio services (T(14)).

To protect against threats, an SDR should be designed with similar mechanisms to the ones adopted to guarantee software assurance in information technology.

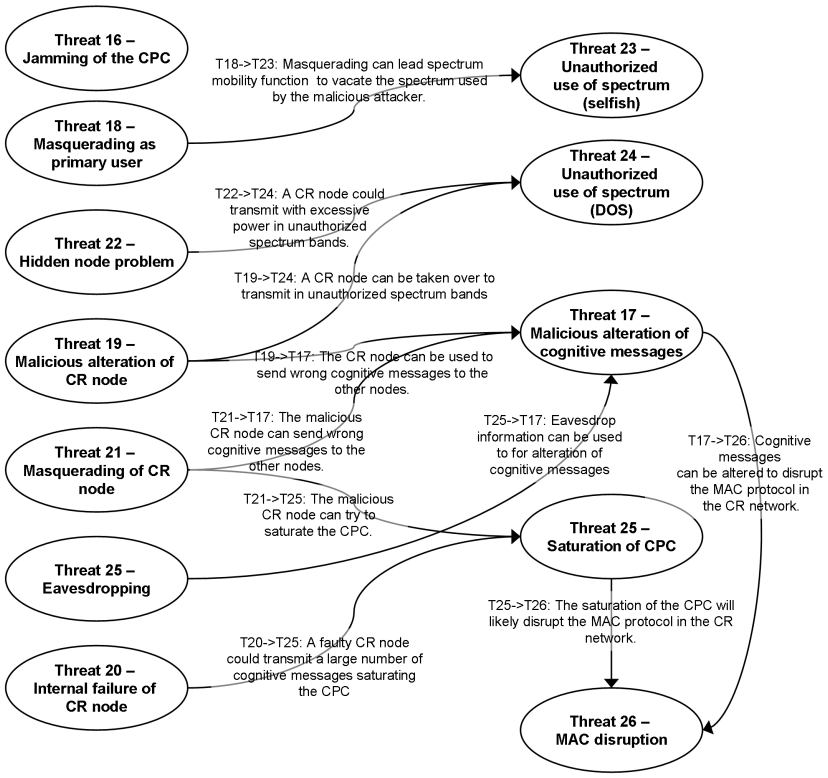

Fig. 6. Relationships among CR threats

Software assurance for SDR requires

- A secure download mechanism, which guarantees the authenticity of the downloaded software. This should be complemented by the components in the SDR terminal to verify the software components.
- A secure execution environment in the SDR terminal to guarantee that only trusted software can be activated and executed. Digital signatures could be used to ensure that only authorized software is activated. Trusted computing could also be proposed.
- A module to ensure that spectrum regulations will be validated regardless of the software modules running on the SDR terminal. Software assurance requires also a complete software certification process, as described in section VII.

These processes and components have already been designed and implemented in various wireless telecommunication systems, but SDR can present unique challenges not addressed in conventional communication technologies.

Mechanisms for secure software download of software modules and upgrades from central servers to BSs have already been implemented in cellular networks for many years. The BSs can be connected to the rest of the network through wireline links or through dedicated wireless links (radio links or satellite) when they are located in remote areas.

Dynamic and secure software download is an important capability of SDR technology. For example, public safety operational scenarios may require the reprogramming of SDR terminals during an emergency due to unexpected requests or changes in the operational context.

SDR technology presents the following challenges in comparison to conventional systems:

1) SDR may use wireless links and technologies, which may not have been designed for secure software download.
2) The computing and processing power of a mobile SDR terminal may be limited in comparison to a BS. Security mechanisms should consider this design constraint.
3) The downloaded software modules must be consistent with the regulations in the area, where the terminal is operating. An SDR terminal may roam to an area where the original software configuration is not correct and a new software module must be downloaded. This requirement is particularly important in border security operations across different member states or emergency crisis, which spans more than one jurisdiction. In the commercial domain, an SDR terminal must also be automatically reconfigured when it moves from one geopolitical area to another where the spectrum regulations are different (e.g., Europe or USA).
4) In specific domains (e.g., military, public safety), the CR networks must support different levels of security: this is the concept of multiple independent levels of security/safety (MILS), where parties exchange voice and data at different levels of security. Currently, MILS is a concept mainly proposed in the military domain, but it is difficult to deploy it in the commercial domain for cost reasons.

Summarizing the previous considerations, we can classify the protection techniques against the SDR security threats in the following categories:

1) Protection techniques for secure software download (T(1) and T(13)).
2) Protection techniques to ensure a secure execution environment (T(2), T(3), T(4), T(5), T(6), and T(7)).
3) Protection techniques for conformance to regulations (T(14)).
4) Protection techniques for high availability (T(8) and T(9)).
5) Data assurance (T(10), T(11), T(12), and T(15))

1) Protection techniques for secure software download (T(1) and T(13)):

The use of digital signatures to prevent activation of unauthorized software is described in [20], [49], and [50].

The proposed security framework is based on a public/private key scheme for the authentication and verification of software. As described in [20], the manufacturer generates a digital signature of the software waveform after certification, which is usually implemented as a hash and an encryption function. The digital signature is then added to the software file of the waveform. The software file is then encrypted with a secret key, which is unique to each terminal. That is, only that terminal has the knowledge of the secret key. The secret key is stored in tamperproof hardware on the terminal device. Since symmetric encryption techniques are used, encryption and decryption is fast. The software waveform file is then released for deployment in the network.

The framework describes also the roles of the main stakeholders including the government, the manufacturer of the SDR terminal, the producer of the software components, and the wireless provider. This solution has the advantage that the regulatory agencies can control the approval of software and/or software/hardware combinations.

The disadvantage is the complexity of the framework because digital signatures should be created for all the combinations of software waveform/terminals, and digital signatures must be reissued every time a new version of the software waveform is created. Furthermore, a process for the removal or update of secret keys should also be established.

An alternative mechanism for secure download is described in reference [48], which uses the characteristics of the field programmable gate arrays (FPGAs) composing the SDR. The wiring of configuration logic blocks on FPGAs can be arranged in many different ways enabling high-security encipherment to prevent illegal acquisition of software using replay attack. This approach assumes that the SDR devices download software only from the SDR terminal manufacturers, which is a strong limit for the SDR business model. Finally, [50] discusses the market drives and requirements for software download but security aspects are not considered.

Reference [47] addresses the challenge of implementing a security mechanism, which takes into consideration the limited computing and processing power of a mobile SDR terminal. The paper presents a Light Secure Socket Layer (LSSL) protocol, which is a lightweight version of the Secure Socket Layer (SSL) protocol to ensure the security of the connection used to download the software. LSSL uses less bandwidth and reduces the computational load on the SDR terminal side, transferring the majority of the cryptographic computational intensive operations to the server side. Authentication and data integrity mechanisms are used to ensure the correctness of the downloaded software modules.

As described in some of the references papers, the secure download and activation of software should be based on a comprehensive certification process, where the combination of hardware platforms and software modules must be certified against the spectrum regulation before the deployment. More details on the certification aspects are presented in section VII of this paper.

2) Protection techniques to ensure a secure execution environment (T(2), T(3), T(4), T(5), T(6), and T(7)):

An important aspect of the secure software download is the integrity of the security administrative module (SAM) (e.g., the radio security module described in [22]), which is responsible for download, activation, and execution of the software modules.

The SAM may use security functions on the radio. With the potential harm that malicious SDR code could cause, the veracity of the SAM functions is critical; therefore, these functions must be implemented with a suitable level of trust. SAM and security functions may even be provided in hardware radio resources. Interfaces to radio resources, which provide security functions, may be public or non-public (just as most current civil wireless systems are largely public with certain security functions kept non-public). This may result in three levels of interfaces and functions for security components: public (for most uses), group managed (for groups of operators, manufacturers, or user communities), and national (government controlled).

This solution will require the implementation of trusted computing (TC) functionality in the SDR and architecture for multilevel security. Reference [51] describes the application of trusted computing to SDR. While TC may not address all the security threats, it could guarantee the secure execution of critical software modules in the SDR terminal. For example, TC could support a secure boot process, which ensures that a set of security-critical platform components boot into the required state.

TC could also protect SDR functions against security threats T(2), T(3), T(4), T(5), and T(6), because the implementation of these threats requires access to specific permission rights, which will be controlled by the TC components.

3) Protection techniques for conformance to regulations (T(14)):

Reference [22] describes a SDR architecture, which is composed of an automatic and calibration unit (ACU), a radio security module, and a location component based on a Global Navigation Satellite System (GNSS) receiver (e.g., GPS). The ACU is responsible for controlling the output spectrum to be compliant with the local spectrum regulations.

The SDR stores the information (e.g., spectrum configuration files) on the spectrum regulations in various spectrum jurisdictions in the world. The GNSS receiver provides the location of the SDR at any given time; the ACU uses the location and the spectrum configuration files to determine the correct spectrum regulations. The ACU represents a protection technique against security threat T(14) if the SDR services are related to transmission and communication of signals. Even if a malicious waveform is activated in the SDR node, the ACU can prevent it from transmitting in unauthorized bands.

A similar solution is also presented in [100], where a policy manager and policy enforcer are used to restrict the access of the SDR/CR node to the spectrum by ensuring that the SDR/CR configuration conforms with regulatory and system policies.

4) Data assurance (T(10), T(11), T(12), and T(15)):

Security threats against loss, alteration, eavesdropping of data (threats T(10), T(11), T(12), and T(15)) can be mitigated by applying data protection and data integrity guidelines (see [16]) and techniques (see [17]), which have already been developed in the computing world for real-time systems. Usually, this is the task of the RTOS in the SDR.

5) Protection techniques for high availability (T(8) and T(9)):

High assurance (HA) solutions could be used to counter security threats T(8) and T(9) due to an internal failure. High assurance for SDR is discussed in [14] and [54], and many SDR manufacturers are proposing HA solutions mostly for the military market. Reference [54] describes the high assurance wireless communication system (HAWCS), which is a set of security components to provide higher HA and security to the SDR platform and waveforms.

Finally, the MILS concept and solutions are described in [52] and [53]. The proposed solutions are not designed specifically for SDR, but they could be tailored to the SDR architecture. The implementation of MILS address also threats T(2), T(7), T(14), and T(15), because elements with a lower level of security may access and modify data or modules at a higher level of security. The implementation of MILS is necessary in the military and public safety domains, (less in the commercial domain) but its implementation can be quite complex and it may increase the price of the SDR equipment. As described in [52] and [53], MILS requires the implementation of partitions for memory and communication channels, which increases the complexity of the SDR architecture and requires multiple components for all the security levels.

The research status of this area seems mature and many papers have provided a complete framework to ensure secure software download and execution on an SDR. A significant challenge is the complexity of the framework, which involves various stakeholders and a high level of control over the certification and deployment procedures. These procedures can be simplified if the software modules are produced by the SDR hardware manufacturers, but this approach would invalidate the business model of software portability. Another challenge is the cost impact of the security solutions, which may not feasible for the commercial domain.

B. Cognitive Radio Protection techniques

As described in section IV, masquerading attacks and the distribution of false information in cooperative CR networks in relation to CR functions (i.e., spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility) are perceived by the research community as the most significant threats to CR. In this paper, these threats are identified by T(17), T(18), T(19), and T(21). In the current collaborative sensing schemes, secondary users are usually assumed to be trustworthy. Such schemes may fail in the presence of a masquerading threat. A number of protection techniques have been proposed by various authors to address such threats and improve the robustness of collaborative sensing algorithms.

We can classify the protection techniques against these types of threats in the following categories:

1) Protection techniques based on reputation and trust of the CR nodes.
2) Identification of the masquerading threat though signal analysis.
3) Authentication of the CR node through cryptographic techniques.
4) Geolocation database of primary users.

1) Protection techniques against security threats T(17), T(18), T(19), and T(21) :

Protection techniques based on reputation and trust of the CR nodes.

A number of protection techniques are based on the concepts of reputation or trust of the CR nodes (BS or terminals). For example, in the spectrum sensing function, a CR node can be classified at different levels of reputation or trust on the basis of spectrum sensing information, which they provide to the other nodes in the CR network. If the information is not correct after a number of iterations, then the contribution of that specific CR node is considered not valid, which may hint to a security threat by a malicious CR node. Protection techniques based on reputation or trust are presented in [55] and [56] for cooperative spectrum sensing.

References [33], [38], and [57] propose a trust decision algorithm to detect both single ([33]) and multiple attacks ([38] and [57]) in a centralized cooperative sensing architecture. The complexity of the detection algorithm for multiple attacks can become unpractical in the case of a large number of nodes in the cognitive network. To simplify the problem, an "onion-peeling approach" is presented, where all the CR nodes are initially considered honest, and they are considered malicious when a specific threshold is overcome.

Comprehensive simulations are conducted to study the receiver operating characteristic (ROC) curves and suspicious level dynamics for different attack models, attacker numbers, and different collaborative sensing schemes. This approach has been extended in [42], where an abnormality detection based

algorithm is used for the detection of attackers in collaborative spectrum sensing. The novelty of the paper is that it does not assume any a priori information about the strategy of attackers. In [58], the average power obtained from real-valued reports is used for the decision of spectrum sensing, and attacker detection is carried out using a trust factor scheme.

In [39], a technique called weighted sequential probability ratio test (WSPRT) is proposed to address Byzantine failures (threats T(18), T(19), T(20), and T(21)) in the data fusion process of collaborative spectrum sensing. A reputation rating is allocated to each terminal based on the consistency of its local sensing report with the final decision. This approach addresses both masquerading attacks and general failure of the CR node.

A cross-layer approach to address Byzantine failures is described in [59], which shows that a centralized cooperative architecture is more efficient in addressing these types of security threats.

Reference [60] shows that over a certain fraction of Byzantine attackers in the CR network, the reputation data fusion scheme becomes completely incapable, and no performance gain can be achieved.

Reference [61] proposes an improvement of the collaborative spectrum sensing algorithm with an energy detector with double thresholds combined with revised data fusion rules to find untrusted CR nodes.

Reference [62] proposes a consensus algorithm that has taken inspiration from the self-organizing behavior of animal groups. The algorithm is applied to CR mobile ad hoc networks, where a centralized authority is missing and the conventional spectrum decision algorithms may not be applicable. The consensus algorithm addresses threats T(17), T(18), and T(21).

Identification of the masquerading threat through signal analysis

This protection technique is based on signal analysis to distinguish a malicious attacker from a licensed user. This technique is mainly used to address threat T(18), where a malicious attacker can "masquerade" as an incumbent transmitter by transmitting unrecognizable signals in one of the licensed bands, thus preventing other secondary users from accessing that band. A wide range of spectrum sensing techniques are available as described in [63], and they include power sensing, matched filter, and cyclostationary feature detection. A protection technique against threat T(18) for collaborative sensing is proposed in [64], where a transmitter verification procedure is described. The transmitter verification procedure employs a location verification scheme to distinguish incumbent signals from unlicensed signals masquerading as incumbent signals. Two alternative techniques are proposed to realize location verification: distance ratio test (DRT), which utilizes the received signal strength (RSS) of a signal source, and distance difference test (DDT), which relies on the received signal's relative phase difference when the signal is received at different receivers. The paper assumes the presence of location verifiers (LVs), which are CR nodes with a known position (because fixed or using trusted GPS) and which perform DRT and DDT in the coverage area of responsibility. LVs know also the location of the incumbent transmitter and they can exchange information through a cognitive pilot channel. A major problem for DRT is the difference in the radio propagation paths among LVs, which can undermine the identification of the attackers. This is especially critical in urban environments, where buildings and other obstacles generate multipath fading. As a consequence, DDT is the preferred technique to identify a security threat.

The DDT is based on the embedded synchronization pulses of TV signals. The proposed protection technique has three challenges:

1) The LVs must be time synchronized, which could be expensive to implement.
2) The DDT is based on the synchronization pulses of the TV signals, which is only one of the incumbent signals.
3) The algorithm is based on the large difference in transmission power between the incumbent TV transmitter and the hand-held terminal user. In ad hoc cognitive networks, the difference in transmission power would not be so high.

The paper describes also a public-key cryptosystem for the secure exchange of CR messages to mitigate threats T(17) and T(26). In [65], the authors present a cooperative detection scheme with malicious user suppression. The scheme is based on collaborative secondary users, which exchange and implement decision fusion on local decision results instead of detected energy. The scheme is based on weighted coefficients, which are updated recursively according to the deviations between separate decision information and the combining results.

Reference [66] describes the concept of the radio environment map (REM), which is envisioned as an integrated database that consists of comprehensive information like geographical features, available services, spectral regulations, locations, and activities of radio devices and policies. LVs could use this information to detect masquerading threats like T(18) or spectrum regulatory breaches like T(24). The challenge of this protection technique is the complexity of the distribution and synchronization of the information across the LVs in the network. For the protection technique to be effective, the LVs should be continuously updated with the latest version of the REM, which could overcome the limits of the traffic capacity of the cognitive pilot channel and indirectly induce threat T(25).

Identification of a CR node through an analysis of the transmitted signal is investigated in [67], where wavelet transform is used to magnify the characteristics of transmitter fingerprints. The challenge of this protection technique is that radio propagation errors or effects could increase the probability of false alarms. An attacker could also try to emulate the transmitter fingerprints.

In [68], the authors propose a waveform pattern recognition scheme to identify emitters and detect camouflaging attackers by using the electromagnetic signature (EMS) of the transceiver. The EMS is based on the distinctive behavior present in the waveform emitted by the components of the transceiver, including frequency synthesis systems, modulator subsystems, and RF amplifiers. The issue with this approach is that the EMS may change with the aging of the transceiver.

It would be also difficult to keep an EMS inventory of all the devices in operation.

Sophisticated signal processing algorithms like cyclostationary analysis, classification engines, or signal feature extraction (in the time or frequency domain) are also explored in [36]. The paper presents the results of simulations, which show that these algorithms could be quite effective in identifying a false signal. The paper concludes that the ideal solution is to develop a classification system with robust and unique signal features that are difficult to emulate. Unfortunately, analyzing these features is typically too complex to do in real time with commercial wireless device hardware. In the following work [36], the authors have investigated the use of unsupervised learning in signal classifiers, and attacks against self-organizing maps. By temporarily manipulating their signals, attackers can cause other secondary users to permanently misclassify them as primary users, giving them complete access to the spectrum.

Authentication of the CR node through cryptographic techniques

A number of papers have proposed authentication of CR nodes based on similar mechanisms already defined for other types of wireless networks like ad hoc networks [29]. The challenge of this approach is that SDR/CR should be able to interface with a variety of communication systems and satisfy different security requirements. The authentication procedures defined for a specific communication network (e.g., UMTS) may not be apt for SDR/CR networks. The authentication mechanism should be extendible to all the communication systems with which the CR nodes have to interface.

In [69] is presented an authentication protocol for CR networks that can be integrated with the Extensible Authentication Protocol (EAP). The protocol allows quick radio switchover in CR networks without the need to consult an AAA (e.g., Authentication, Authorization and Accounting) server for re-authentication.

Authentication protocols for CR networks may have different implementations depending on the CR architecture. A centralized CR architecture can adopt authentication mechanisms based on a central certification authority (CA) for key management, while a distributed architecture could relay on solutions for distributed mobile ad hoc networks (MANETs) as described in [70]. One example of key management algorithms for a distributed MANET is described in [71] for Pretty Good Privacy (PGP)-like algorithms, where each node is responsible for creating its public and private keys. In this system, key authentication is performed via chains of public key certificates.

In [72], the authors propose an efficient and provably secure protocol that can be used to protect the spectrum decision process against a malicious adversary. The protocol is based on a clustered infrastructure-based dynamic spectrum access network where the spectrum decision in each cluster is coordinated by some central authority.

Beyond authentication, CRN should also ensure authorization of the cognitive nodes to transmit in specific spectrum bands or perform specific functions. The authorization is often conditional to the nature of the spectrum environment, i.e., the presence of primary users in the area. The authorization is needed to define the roles of CR nodes in the CR functions defined in section II.

For both authentication and authorization, we assume that CR nodes may exchange authentication information (e.g., certificates) through a common channel, which could be the CCC itself. A framework to protect the exchange of information on the CCC is described in [73].

Geolocation database of primary users

In the geolocation database approach, the CR network provider maintains a database with the position and transmission features (e.g., power) of all the primary users in the area. The CR geo-locates itself though the GNSS (e.g., GPS) and compares the data received from the spectrum sensing functionality with the known position of the primary users. A mismatch may indicate a malicious attacker. The database of the primary users can be downloaded periodically from a server. The position of the primary users' emitters does not change very frequently (e.g., in the order of months), so the database updates and related CR node synchronization will not have an impact on the performance of the system. This approach is described in [26] and [89]. In comparison to other protection techniques, this approach is relatively simple to implement as the spectrum sensing functions in the CR node do not have to be very sophisticated. Obviously, the approach is vulnerable to GNSS security attacks (e.g., spoofing) or lack of GNSS availability, especially in urban environments (e.g., urban canyons). Reference [89] proposes also a protection technique based on a beacon, where a primary user would transmit a beacon to alert any secondary users to not transmit in specific spectrum bands. The disadvantage of this solution is that primary users should modify their equipment to provide the beacon transmission.

2) Protection techniques to increase the robustness of the cognitive control channel: jamming (T(16)) and saturation (T(25)) :

The cognitive pilot channel (CPC) is a potential vulnerability of a CR network. As described in section IV, CR networks can be based on the concept of CPC, which is responsible for distributing the cognitive control messages to support the CR functions. The CPC is subject to threats T(16) (DoS through jamming) and T(25) (saturation). Virtually any wireless system is vulnerable to brute force DoS attack through jamming, but a CR network based on a single CPC channel allocated to a specific spectrum band is particularly vulnerable to jamming attacks in that band.

A protection technique against a jamming attack in a specific spectrum band (i.e., T(16)) is based on frequency hopping. The CPC could use more than one spectrum band and "hop" among the spectrum bands to avoid a jamming attack. The trade-off is an increased complexity of the CR network as the CR nodes should be notified about the change in the frequency band of the CPC. If the attacker monitors the CPC, it could "chase" the CPC band for every change and eventually cause continual adaptation and outage of service to the CR network. Another issue is the need to allocate various

spectrum bands for CPC, which may not be acceptable by spectrum regulators.

Another protection technique for T(16) is described in [74] and [75], where rateless coding and piecewise coding are used to mitigate jamming attacks in CR networks. While the paper applies the technique to the secondary users, it can also be used for the CPC itself.

Reference [76] describes a lightweight mechanism for a secure physical (PHY) layer in CR networks using orthogonal frequency division multiplexing (OFDM). The idea is to secure the PHY layer with a random and dynamic sub-carrier permutation, which is based on single pre-shared information and depends on dynamic spectrum access (DSA).

Narrowband jamming attacks could also be mitigated by using ultrawideband (UWB) CCC, with very wide spectrum occupancy. This solution can increase the complexity of CR nodes as it should support conventional narrowband wireless communication systems and the UWB CCC. Furthermore, there could be interference issues between the UWB CCC and the primary users.

3) Protection techniques for unauthorized use of the spectrum: security threats T(23) and T(24) :

Threats T(23) and T(24) in relation to the unauthorized use of the spectrum are investigated in [85], which presents a framework to guarantee that CR nodes behave according to acceptable communal spectrum policies. The framework is based on a TC base/module in the CR node, which enforces the policy rules defined in the XG Policy Language (XGPL) to express spectrum policies formally.

Another approach to mitigate threats T(23) and T(24) is presented in [87], which proposes a mechanism based on the estimate of the level of interference created by secondary users. The paper suggests a hardware implementation, which is not vulnerable to threats to the software waveforms and framework (threats T(1), T(4), T(5), T(6), T(8), and T(13)).

An alternative protection technique to address threats T(23) and T(24) is the deployment of spectrum monitoring systems, which act as a spectrum "watchguard" to identify the misuse of the spectrum.

The spectrum monitoring systems should provide the following functions:

1) Monitoring of the spectrum usage in a specific spatial region and range of frequencies.
2) Identification of wireless services and their sources.

The design of an effective spectrum monitoring system can be difficult for a number of reasons. We can identify the following challenges:

1) Natural or man-made obstacles can change the features of the radio signal. If the spectrum monitoring system is located only in one location, its measurements may not be complete or valid in the area of competence.
2) Identification of wireless services may not be easy if the attacker tries to emulate a specific wireless service. Sophisticated spectrum sensing techniques may be needed to identify malicious attackers as described in the previous sections.
3) A spectrum monitoring system has associated costs for design and deployment.

There are a number of solutions to address the above challenges. The spectrum monitoring systems could be distributed across the users themselves. After all, CR nodes should have spectrum sensing capability to detect the spectrum usage and other wireless services in the area. Information on the wireless services in the area could be transmitted to a central monitoring location, which could correlate the various inputs and check the received information against other data like the known position of the wireless services in the area and their source or emissions (e.g., main transmitters for digital TV broadcasters or 3GPP BSs).

The main problem of this approach is that the spectrum sensing capabilities and the amount of data, which can be transmitted by the users' devices, could be of limited value because of various constraints, mainly defined by business reasons. The transmission of data for monitoring purposes has an associated cost on the uplink channels of the CR devices. Furthermore, the implementation of sophisticated spectrum sensing and identification algorithms in the user's devices may not be cost effective for device manufacturers.

A hybrid solution could be based on a limited number of monitoring stations in the area, which receive limited data from the user's devices and use it to perform a more sophisticated analysis of the spectrum.

Once the spectrum monitoring system has detected a malicious or misbehaving CR node, an administrative mechanism should be implemented to shut down the offending node. In most cases, this requires a centralized authority, which has the right to shut down any CR nodes in the area of responsibility.

In [77], the authors present a model to define an enforcement structure to deter malicious attacks. The model uses administrative commands to "shut down" a CR, which has been identified as malicious or misbehaving against the spectrum policy rules. The model is based on an identity system described in [78].

4) Protection techniques against hidden node problem: T(22) :

Protection techniques against the hidden node problem have been extensively researched in literature. The most common approach is based on collaborative sensing to identify the incorrect spectrum perception of the affected CR node. This is the approach adopted in standard IEEE 802.22 [44], where decision rules (e.g., voting algorithm) are used to correct errors in the spectrum sensing function. In a similar way, this approach is also described in [34], even if the term distributed spectrum sensing is used.

In [94], the author proposes the combination of the integral equation based propagation method with the REM concept described in [66]. The idea is to use the REM to predict the "shadow" areas where the CR node may not determine correctly the signal of the primary user.

Finally, [97] presents a new approach based on a satellite assisted CR network, where a low equatorial orbit (LEO) satellite is the central spectrum controller, which collects the spectrum occupancy maps for each CR BS. Due to the

wide satellite coverage, this approach is able to identify inconsistencies on a large area. The paper also addresses mobility aspects related to the handover of CR nodes from one CR BS to another.

5) Protection techniques against threat T(27):

Protection techniques against threats to the MAC, network layer, or the cognitive engine are usually based on a robust design. A Survey on MAC Strategies for cognitive

radio networks is presented

As described in section VI, the 802.22 standard defines an authentication and encryption scheme to mitigate attacks against the MAC.

In [100], the authors propose two protection techniques against threats to the cognitive engine:

1) The likely effect of a threat is to disrupt the state machine and bring the CR device to an incorrect state. Formal state-space validation, as is often done with cryptographic network protocols, can be applied to the state machine to ensure that a "bad state" is never reached.
2) The beliefs of the cognitive engine should be constantly re-evaluated and compared to a-priory knowledge (e.g., local spectrum regulations) or rules (e.g., relationships among power, propagation, and frequency).

At the level of the CR network, reputation and trust schemes, already presented in previous sections, can be used to identify and deny access to a CR node, whose cognitive engine is not working properly.

Table III and IV provide a summary of the protection techniques described in this section and how they address the security threats.

TABLE III
PROTECTION TECHNIQUES FOR SOFTWARE DEFINED RADIO

Threat ID	Threat Description	Protection Techniques
T(1)	Insertion of malicious software	Use of digital signatures for software modules, Trusted computing
T(2)	Alteration or destruction of the configuration data	Data integrity functionality in the RTOS or Software Framework (Middleware)
T(3)	Artificial consumption of resources	Trusted computing, RTOS watchdog
T(4)	Alteration or destruction of waveform code	Use of digital signatures for software modules, Trusted computing, Use of secure administrative module (SAM)
T(5)	Destruction or alteration of real-time operating system software	Trusted computing
T(6)	Alteration or destruction of the software framework	Trusted computing
T(7)	Alteration or destruction of user data	Data integrity functionality in the RTOS or Software Framework (Middleware)
T(8)	Software failure	High assurance techniques
T(9)	Hardware failure	High assurance techniques
T(10)	Extraction of configuration data	Data integrity functionality in the RTOS or Software Framework of the SDR platform
T(11)	Extraction of waveform data	Data integrity functionality in the RTOS or Software Framework of the SDR platform
T(12)	Extraction of user data	Data integrity functionality in the RTOS or Software Framework of the SDR platform
T(13)	Masquerading as authorized software waveform	Use of digital signatures for software modules, Trusted computing
T(14)	Unauthorized use of software defined radio services	Use of secure administrative module (SAM) and automatic and calibration unit (ACU)
T(15)	Data repudiation	Data integrity functionality in the RTOS or Software Framework of the SDR platform

VI. SECURITY ASPECTS IN SDR/CR STANDARDS

The purpose of this paragraph is to describe how security aspects are investigated in the following standardization bodies and fora:

1) Wireless Innovation Forum
2) IEEE 802.22
3) IEEE SCC41
4) ETSI TC RRS

These are the main organizations that are working on SDR/CR standards and where security aspects have been addressed. Some of the protection techniques described in the previous chapters may be presented again in this paragraph in the context of a specific standard.

The Wireless Innovation Forum did significant work in the area of security for CR and SDR. One of the very recent achievements is the technical report on securing software reconfigurable communications devices [88]. This document provides design and manufacturing process guidance regarding security solutions for software reconfigurable radio platforms. Topics covered include analysis of potential vulnerabilities, threats, attacks/exploits, and associated risk analyses. The document also provides guidelines for developing the radio platform security policy and describe security services and mechanisms needed to implement the radio platform security policy. Included are discussions on developing a security architecture that integrates the security services so that the radio platform security policy is always enforced. The document includes a representative set of requirements as well as references to other standards and references that manufacturers can consider for use in their products. In the WINNF (Security Services API Task Group), a project has been started to develop structures, guiding principles, requirements, and definitions of security service interfaces for SDRs.

TABLE IV
PROTECTION TECHNIQUES FOR COGNITIVE RADIO

T(16)	Jamming of the channel used to distribute cognitive messages	Frequency hopping
T(17)	Malicious alteration of cognitive messages	Protection techniques based on trust or reputation, Identification of masquerading threats through signal analysis, Authentication of CR nodes
T(18)	Masquerading of a primary user	Protection techniques based on trust or reputation, Identification of masquerading threats through signal analysis, Authentication of CR nodes
T(19)	Malicious alteration of a CR node	Protection techniques based on trust or reputation, Identification of masquerading threats through signal analysis, Authentication of CR nodes
T(20)	Internal failure of a CR node	Data fusion process of collaborative spectrum sensing
T(21)	Masquerading of a CR node	Protection techniques based on trust or reputation, Identification of masquerading threats through signal analysis, Authentication of CR nodes
T(22)	Hidden node problem	Data fusion process of collaborative spectrum sensing
T(23)	Unauthorized use of spectrum bands for selfish use	Framework to enforce spectrum policies
T(24)	Unauthorized use of spectrum bands for DoS to primary users	Framework to enforce spectrum policies
T(25)	Saturation of the cognitive control channel	Robustness, Protection of system integrity
T(26)	Eavesdropping of cognitive messages	Protection of confidentiality
T(27)	Disruption to the MAC of the CR network	Verification of identities, Controlled access to resources, Protection of system integrity

IEEE 802.22 [91] was one the first standards for CR. Reference [90] explains that standard 802.22 is aimed at using CR techniques to allow sharing of a geographically unused spectrum allocated to the television broadcast service, on a noninterfering basis, to bring broadband access to rural environments. IEEE 802.22 WRANs are designed to operate in the TV broadcast bands while ensuring that no harmful interference is caused to the incumbent operation (i.e., digital TV and analog TV broadcasting) and low-power licensed devices such as wireless microphones.

References [44] and [93] describe the reference architecture of 802.22, which is composed of two security sublayers for non-cognitive and cognitive security mechanisms.

The IEEE 802.22 security sub-layer 1 provides the non-cognitive security mechanism to ensure availability, authentication, authorization, identification, data integrity, confidentiality, and privacy. Several parts of the key management Version 1 (PKMv1) along with parts of PKMv2 used in IEEE 802:16, have formed the secure management protocol (SCM) used by IEEE 802:22.The security suite also consists of authorization and authentication processes. The authorization process is carried out at the time of network entry to ensure that only authorized devices can access the network. A CR BS is capable of de-authorizing customer premise equipment (CPE) or CR terminal if it finds that it does not contain valid authorization keys or it is generating spurious emissions. As a consequence, the proposed solution addresses security threats T(19), T(21), T(23), and T(24). The authorization process also includes an authentication process where both the BS and the CPE can authenticate each other. Once a CPE has completed authorization, it has keying material that can be used to sign and/or encrypt further MAC management messages. This proposed solution addresses CR security threats T(17), T(26), and T(27).

The IEEE 802.22 security sub-layer 2 provides the cognitive security mechanism, which implements collaborative sensing, signal classification, correlation with geolocation information, and decision-making. In collaborative sensing, the local sensing information is combined with information from the incumbent database to see if any of the CPEs lie in the protected contour of an incumbent. Collaborative sensing can use a voting rule, where a CR terminal can vote to identify a malicious CR node or the case of a hidden CR node. The security sub-layer 2 addresses security threats T(18) and T(22).

The Technical Committee (TC) on reconfigurable radio systems (RRSs) is responsible for the standardization of SDR and CR technologies in ETSI. The activities of ETSI TC RRS are presented in [7]. SDR-related study results are presented with a focus on SDR architectures for mobile devices (MD) (e.g., mobile phones). CR principles within ETSI RRS are concentrated on two topics, a CPC proposal and a functional architecture (FA) for management and control of reconfigurable radio systems.

Security aspects have been investigated in Working Group 4 for the specific public safety domain. From 2011, research on security threats and solutions will be extended to the commercial domain as well in the areas of secure software download and security of the CCC.

IEEE Standardization Coordinating Committee 41, "Dynamic Spectrum Access Networks." The objective of IEEE SCC41 is to develop standards supporting new technologies for next-generation radio and advanced spectrum management. Security is considered an important area to investigate, and there are still open issues to be resolved. In [96], the following security design issues are considered: secure primary user (PU) detection, resilience to non-jamming DoS attacks on the secondary user (SU), and DoS attacks on the primary network.

VII. SECURITY EVALUATION AND CERTIFICATION

The introduction of SDR and CR technologies will introduce new evaluation and certification issues, unlike those faced by conventional wireless communication systems. Because software changes in the SDR can alter the radio behavior, a certification authority must certify not only the hardware and

radio equipment platform but also the software waveforms and components of the framework. In comparison to conventional radio systems, the certification process should also address the portability of the waveforms (including security mechanisms for data COMSEC and TRANSEC). A software waveform can be installed and activated on different platforms, which can support the waveform execution. As described in the previous sections, software portability shall include security mechanisms, which guarantee the authenticity of the waveform and that the SDR platform can be trusted.

The certification process is based on evaluation and certification criteria, which are defined on the basis of regulations, standards, and industry specifications.

These criteria have to be partially adapted to the new complex features of SDR and CR. There are usually two certification processes: one process to certify the SDR platform, which includes the HW platform, RTOS, and software framework; and the second process for waveform certification. Additionally, a certification process should be established for the security requirements and threats presented in this paper. The security evaluation and certification process of SDR can be based on similar processes already defined in information technology, like the common criteria [87]. Among other things, common criteria allow us to define protection profiles, which identify the security requirements, and assurance levels for classes of products (i.e., SDR) or components of them. Based on these general protection profiles for each SDR, a security target has to be generated, against which the product can be evaluated. This model is appropriate for the future use of SDR in different markets: military, public safety, and commercial, with different security requirements and equipment costs. For every corresponding product (SDR), a protection profile could be developed to support the standardization of security evaluation and certification. As described in [79], the security certification process is particularly complex for SDR equipment because of the complexity of the technology and because various stakeholders could be involved in the certification process. In comparison to the security evaluation and certification process based on common criteria, SDR/CR devices should be evaluated for compliance to spectrum regulations and against the security threats described in section IV. As a consequence, new relationships among spectrum regulators, equipment providers, certification organizations, and security authorities should be created.

The certification of SDR is particularly complex in the European context, where spectrum allocations could be different among member states and central certification and security authorities are missing. In the USA, SDR certification organizations are already defined, like the JPEO, which is the certification authority for compliance to the SCA in the military domain. As a consequence, the SDR certification processes in the USA and Europe can have different evolutions.

Test organizations can be certified as test and evaluation authority (TEA). In the commercial domain, the FCC established in [81] that radio equipment, which has SW that affects the RF operating parameters, is required to be certified. As described in [19], the certification is required to be carried out in FCC labs; no self-certification or certification by telecommunications certification bodies (TCBs) is allowed.

In Europe, the situation is slightly different. SDR certification has been investigated in two framework program projects: FP6 WINTSEC project [80] and FP7 EULER project [82].

The FP6 WINTSEC project [80] has concentrated on the aspects of architecture certification and has proposed the creation of a networked certification test bed, where certification centers across Europe are coordinated by a central authority. The centralized certification authority would not execute actual certification of products; instead, it would prepare, monitor, and accredit the certification centers. Location transparency of the certification process would be necessary, which means that it should not be easier to pass certification at one center rather than another. The networked certification center should also be supported by a set of distributed testing tools.

The WINTSEC project also proposed the concept of "waveform libraries," which is a common, centralized repository (called "Waveform Repository") of all the waveforms that have passed the required certifications. This would facilitate over-the-air (OTA) downloads of waveforms as well as upgrades of waveforms and components. The repository could be used to mark the certified waveforms with the digital signatures as described in section V. The repository would be a valuable tool during the certification process, by storing the results of the tests and keeping a history of past certifications.

In the European context, the waveform repository could have a distributed, redundant architecture, with one central European instance and replicated repositories in the European member states maintained by a national authority. 7 shows the relationships of the waveform repository with users, developer, and owner of the waveforms.

However, published standards are needed for certification. The guidelines described in the deliverables of the WINTSEC project are designed against a future, European Software Radio Architecture (ESRA) SDR standard and they are described as "compliance evaluation procedures" rather than "certification procedures."

The WINTSEC project has laid the foundations of ESRA, which, however, has not yet reached the level of a standard but rather an architectural framework; the items defined in the ESRA document are not actual requirements but mere recommendations. The ongoing EULER project, which is expected to provide further ESRA recommendations extensions, will also not propose an SDR standard.

As described in [83], the concept of compliance evaluation is significantly less rigid than that of certification evaluation for a number of reasons: a) compliance evaluation is a much more informal, less authoritative procedure where the steps and requirements can be adapted to each specific test case; b) compliance evaluation can be performed on any relatively mature version of the product under test as it deals mostly with general properties of it, rather than specific details; c) the result of compliance evaluation is a report elaborating on the estimate of each property's compliance to the guidelines; d) compliance evaluation procedures are often related to new, rapidly evolving technological domains, where a standard and certification evaluation procedure would quickly become outdated or hinder development.

It is advisable that a set of guidelines/directives accompanied by compliance evaluation procedures evolves into a

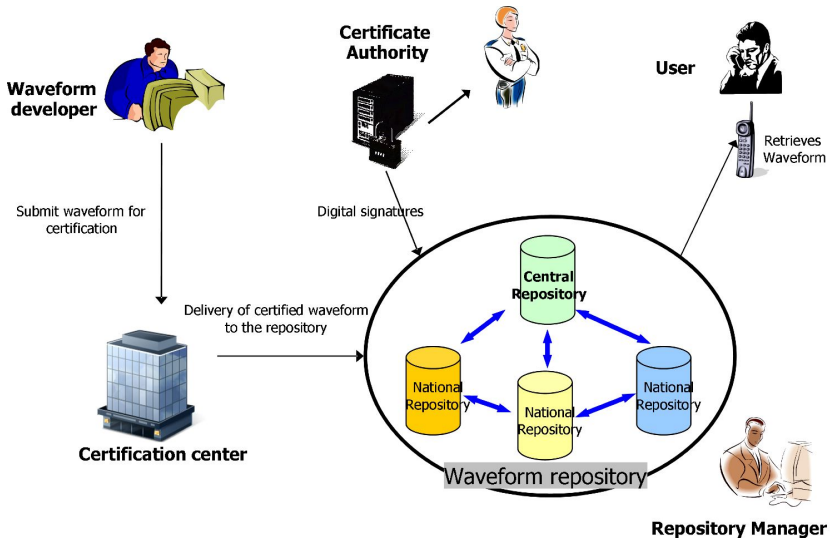

Fig. 7. Waveform repository

standard and certification evaluation procedure as the technological domain involved matures.

VIII. Summarizing The Challenges-The Way Ahead

The goal of provisioning Information Assurance (IA) and the appropriate level of security for SDR and CR networks implies that many issues and challenges exist, and a given solution will be regularly in need of review and updating. IA for SDR and CR networks shall always be topical by virtue of the benefits in spectrum flexibility (such as, mobile high-capacity dynamic communication resources) offered to end users of authorized networks, and therefore, simultaneously, the opportunity to intercept and disrupt the communications networks by the malicious or unauthorized community. This challenge of provisioning assurance exists in the wired world, and the threat to national security and commercial activity has mandated greater attention by various national agencies to Cyber-security. Therefore, in much the same way that the IP infrastructure supplied ubiquity to computer networks in predominantly wired environments (from application layer to the networking layer), the correct utilization of SDR and CR networking shall supply ubiquity to communications and networking infrastructures in wireless environments (from application layer to the physical layer).

These arguments therefore present potentially three core groups of issues and challenges:

1) SDR and CR network related issues for IA infrastructures.
2) Legacy networking with hybrid SDR and CR IA infrastructures.
3) Next generation wireless IA-enabled ubiquitous communications.

Whilst this paper has focused the attention to the above three challenges in descending level of detail, it is clear to see that with a better control of the issues related to (1) above there is a corresponding need to ensure an efficient integration with legacy systems (2). SDR and CR technologies predicate a need to span security services across the seven ISO layers of the communications and networking stack, which need to exist in the next generation of wireless systems and networks. Therefore, this implies that the solutions to (2) will belong to the intermediate stage, as better understanding is gained on the optimal ways to develop waveforms which support (3) in the most efficient way, in terms of strength of IA, ease of monitoring and use, as well as resultant applications and services offered to the end users.

Therefore, if we consider these three core groups, we can readily imagine that the (1) and (2) above extends from opposite ends, and the convergence of which shall yield (3). To this end, the issues and challenges related to cyber security will apply equally to the SDR and CR networked infrastructures, which support an IP core. Resolving the paradox of ensuring that on the one hand it is possible to rapidly get an assured single logical network assembled, and ensuring that on the other hand equivalent rapid tractability is available shall be essential.

In this context, the definition of realistic operational scenarios for the deployment of SDR/CR technologies is of paramount importance to identify which security threats will be more relevant for the end-users.

If we review again the core group (1) of issues and challenges in SDR/CR technologies, we can identify a number of areas, which have higher priority in the near future.

Among the SDR security threats, the download and activation of malicious software is considered the most important challenge. As described in section V, many research contributions have provided a broad range of technological options, which could be adopted by industry and regulators. In most cases, the described protection techniques may require a complex certification procedure, which guarantees the trust and reliability of the SW (e.g., waveforms) and HW (SDR platform). A certification authority would be responsible for marking the certified waveforms

with the digital signatures. The SDR platform should have an authentication mechanism (as described in section V), which validates the downloaded SW modules. In this area, the biggest challenge is to manage the complexity of the certification and software download process, which can become overwhelming as the number of waveforms and HW platforms increase. Furthermore the certification processes may be different for the military, public safety and commercial domains because of the different operational and business requirements. In the military and public safety domain, any proposed solution should conform and extend the processes and organizational structures already existing for the certification of the equipment and security algorithms (e.g., cryptographic algorithms). In some cases, this framework is already well defined (e.g., JPEO). Furthermore, in these domains, the number of SW and HW manufacturers is relatively limited. In the commercial domain, the certification process should be flexible and scalable to support a large number of manufacturers and SDR software waveforms. A single certification authority may not be appropriate once the SDR/CR market becomes larger. In Europe, there is the additional challenge of creating a security infrastructure for the authenticity of the waveforms, which includes a central authority and national authorities in close collaboration. The role of the main stakeholders in the process should be clearly identified. The stakeholders include the users of the SDR technology, the developers of SW waveforms, the manufacturers of HW platforms, the certification authorities and the government institutions.

A significant challenge for the deployment of security protection techniques in SDR platforms are the real-time requirements for the signal processing, The SDR hardware and waveform code must be fast enough to support the signal input/output rate. Security protection techniques may incur a significant performance penalty in terms of increased runtime overhead and increased memory usage. The performance impact of security protection techniques is an open research area, which requires further study.

As described in the previous sections, a compromised SDR can create harmful interference in unauthorized bands to primary and secondary users. The ACU presented in section V can be an effective solution to enforce the spectrum regulation policies in the SDR device. The spectrum policies can be defined in configuration files accessed by the ACU on the basis of its geographical position. The ACU can be implemented with tamper-resistant hardware and the configuration sets for the spectrum regulations can be installed in the production/certification phase. An alternative or complementary approach is based on a network spectrum monitoring system to check the spectrum environment for malicious attackers, but this solution would not be practical because it would require a considerable deployment effort.

Among the CR security threats, the hidden node problem and masquerading CR attacks including the Primary User Emulation (PUE) are considered the main challenges. A reliable collaborative spectrum sensing function is usually considered the optimal solution for these security threats, but its deployment will be successful only if it does not require algorithms or infrastructures, which are too complex, expensive or not scalable for large networks. The performance impact of security protection techniques based on collaboration sensing should be further investigated. The protection of the spectrum management and spectrum sharing is more complex and requires further research to ensure a secure and reliable distribution of information among the CR nodes in the network. A cross-layer approach may be needed, with the definition of security components in the MAC and network layers of the CR network. The protection techniques should also be linked with the administration functions of the SDR/CR devices and networks: if a malicious node or component is identified, it should be shutdown or blacklisted through the administrative functions. Threats to the cognitive engine are another area, which requires further study. These types of threats are more sophisticated than jamming or PUE attack, but they can be more devastating because they can affect the entire CR network and they will be more difficult to detect.

The definition of security protection techniques in SDR/CR standards is another area with very high priority. The risk is to design SDR/CR standards where security is an afterthought. While IEEE 802.22 includes security sub-layers and security mechanisms are already defined in the Software Communications Architecture (SCA), other standards did not define a comprehensive security framework at this stage.

In summary, we can identify the following areas of interest in the near future:

1) Investigate security issues in the integration of SDR/CR technologies with legacy communication systems. In a second step, investigate the evolution of cyber security in next generation wireless IA-enabled ubiquitous communications.
2) Identify realistic operational scenarios to identify which security threats will be more relevant for the end-users.
3) Investigate the integration of a secure download framework integrated with a comprehensive certification process.
4) Investigate the performance impact of protection security solutions in SDR platform to guarantee that real-time requirements are still validated.
5) Design tamper-resistance modules to enforce the spectrum regulation policies in the SDR device.
6) Investigate the performance and efficiency of protection techniques based on collaborative spectrum sensing for a realistic deployment.
7) Protection techniques for spectrum management and spectrum sharing functions should be further investigated. Link protection techniques with administrative functions of the network.
8) Further research on protection techniques against threats to the cognitive engine is needed.
9) Support the definition of protection techniques in the current standardization activities for SDR and CR.

IX. Conclusions and Future Work

The paper has provided an overview of the security threats and related protection techniques for SDR and CR technologies. Even if this research field is relatively recent, many contributions have already been proposed and a number of protection techniques are identified.

The lack of available spectrum and the simultaneous need to provision increasing number of applications, notably the bandwidth hungry variants, such as real-time video, is a driving force to explore spectrum sharing as an essential element of future wireless systems. As the discussion provided in this paper has indicated, a number of protection mechanisms are key to realizing an assured dynamic spectral environment to benefit the commercial, public-safety and military users.

The exposition herein identifies a range of threats, vulnerabilities, mitigation and protection techniques to support the viable deployment of SDR and CR; this effort requires, as indicated in this paper, further integration between the breadth of activities involved in spectrum regulation, security, certification with a view to harmonize standardization efforts.

Future work will investigate the applicability of these protection techniques to realistic scenarios and how they can be channeled to the standardization activities.

References

[1] J Mitola, "The Software Radio," IEEE National Telesystems Conference, 1992 - Digital Object Identifier 10.1109/NTC.1992.267870.

[2] ETSI - TErms and Definitions Database Interactive (TEDDI) http://webapp.etsi.org/Teddi. Last accessed 29/03/2010.

[3] Wireless Innovation Forum. http://www.wirelessinnovation.org. Last accessed 12/04/2010.

[4] C.R. Aguayo Gonzalez, C.B. Dietrich, and J.H. Reed, "Understanding the software communications architecture," *IEEE Commun. Mag.*, vol.47, no.9, pp.50-57, September 2009.

[5] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: Making software radio more personal," *IEEE Personal Commun. Mag.*, vol. 6, no. 4, 1999.

[6] I. F. Akyildiz, Won-Yeol Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey", *Computer Networks*, Volume 50, Issue 13, 15 September 2006, Pages 2127-2159.

[7] M. Mueck, A. Piipponen, K. Kalliojarvi, G. Dimitrakopoulos, K. Tsagkaris, P. Demestichas, F. Casadevall, J. Perez-Romero, O. Sallent, G. Baldini, S. Filin, H. Harada, M. Debbah, T. Haustein, J. Gebert, B. Deschamps, P. Bender, M. Street, S. Kandeepan, J. Lota, and A. Hayar, "ETSI reconfigurable radio systems: status and future directions on software defined radio and cognitive radio standards," *IEEE Commun. Mag.*, vol.48, no.9, pp.78-86, Sept. 2010.

[8] G. Salami, O. Durowoju, A. Attar, O. Holland, R. Tafazolli, and H. Aghvami, "A Comparison Between the Centralized and Distributed Approaches for Spectrum Management," *IEEE Commun. Surveys Tutorials*, vol.PP, no.99, pp.1-17, 0

[9] NSA's IA Definition, Web-site: http://www.nsa.gov/ia/. Last accessed 4 December 2010).

[10] International Telecommunication Union. Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications.

[11] ITU-T E.408. Telecommunication networks security requirements.

[12] Authorization and Use of Software Defined Radio: First Report and Order. Federal Communications Commission: Washington, D.C., FCC Rcd. 17373, Sept. 2001.

[13] R.C.Reinhart, S.K. Johnson, T.J. Kacpura, C.S. Hall, C.R. Smith, and J. Liebetreu, "Open Architecture Standard for NASA's Software-Defined Space Telecommunications Radio Systems," *Proc. IEEE*, vol.95, no.10, pp.1986-1993, Oct. 2007.

[14] D. Murotake and A. Martin, "System threat analysis for high assurance software defined radios", in *Proceedings, SDR'04 Technical Conference, SDR Forum*, Phoenix, AZ, November 2004.

[15] L. Wenjing and R. Kui, "Security, privacy, and accountability in wireless access networks," *IEEE Wireless Commun.,* vol.16, no.4, pp.80-87, Aug. 2009.

[16] S. Spiekermann and L.F. Cranor, "Engineering Privacy," *IEEE Trans. Softw. Eng.,* vol.35, no.1, pp.67-82, Jan.-Feb. 2009.

[17] M. J. Beller, L. Cheng and Y. Yacobi, "Privacy and Authentication on a Portable Communication System", *IEEE J. Sel. Areas Commun.*, Vol. 11, No. 6, pp. 821-829, Aug. 1993.

[18] R. Hill, S. Myagmar, and R. Campbell, "Threat analysis of GNU software radio," in *Proc. World Wireless Congress*, May 2005, Palo Alto, CA, USA.

[19] T. Ulversoy, "Software Defined Radio: Challenges and Opportunities," *IEEE Commun. Surveys Tutorials,* no.99, pp.1-20.

[20] L. B. Michael, M. J. Mihaljevic, S. Haruyama, and R. Kohno, "A framework for secure download for software-defined radio.", *IEEE Commun. Mag.*, July 2002.

[21] H. Uchikawa, K. Umebayashi, and R. Kohn, "Secure download system based on software defined radio composed of FPGAs.", in *Proc. IEEE International Symposiumon Personal, Indoor and Mobile Radio Communications, (PIMRC 2002)*, vol.1, no., pp. 437- 441, 15-18 Sept. 2002, Lisbon, Portugal.

[22] K. Sakaguchi C. Fung Lam, T. Dzung, D. Munkhtur Togooch, J. Takada, and K. Araki, "ACU and RSM Based Radio Spectrum Management for Realization of Flexible Software Defined Radio". *IEICE Trans. Communications*, Vol. E86-B, No.12, pp. 3417-3424.

[23] A. Brawerman and J.A. Copeland, "An anti-cloning framework for software defined radio mobile devices," in *Proc. IEEE International Conference on Communications (ICC'05)*, vol.5, no., pp. 3434- 3438, 16-20 May 2005, Seoul, Korea.

[24] L. Chunxiao, A. Raghunathan, and N.K. Jha, "An architecture for secure software defined radio," in *Design, Automation & Test in Europe Conference & Exhibition, 2009. DATE '09.* , vol., no., pp.448-453, 20-24 April 2009, Nice, France.

[25] K. Pelechrinis, M. Iliofotou, and V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Commun. Surveys Tutorials*, vol.PP, no.99, pp.1-13, 0

[26] A. Sethi, and T.X. Brown, "Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks," in *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'08),* vol., no., pp.1-12, 14-17 Oct. 2008, Chicago, IL, USA.

[27] Y. Zhang, X. Gaochao, and G. Xiaozhong, "Security Threats in Cognitive Radio Networks," in *10th IEEE International Conference on High Performance Computing and Communications (HPCC '08)*, vol., no., pp. 1036-1041, 25-27 Sept. 2008, Dalian, China 2008.

[28] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis, and G.F. Marias, "Cognitive Spectrum and Its Security Issues," in *The Second International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST '08).*, vol., no., pp.565-570, 16-19 Sept. 2008, Cardiff, UK.

[29] J.L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in *Proc. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM 2008),* vol., no., pp.1-7, 15-17 May 2008, Singapore.

[30] T. X Brown and A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerailities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment," in *Proc. 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM 2007)*, vol., no., pp. 456-464, 1-3 Aug. 2007, Orlando, Florida,

[31] A. Sampath, H. Dai, H. Zheng, and B.Y. Zhao, "Multi-channel Jamming Attacks using Cognitive Radios," in *Proc. of 16th International Conference on Computer Communications and Networks, 2007 (ICCCN 2007)*, vol., no., pp. 352-357, 13-16 Aug. 2007, Honolulu, Hawaii, USA.

[32] J.L. Burbank, A.R. Hammons, and S.D. Jones, "A common lexicon and design issues surrounding cognitive radio networks operating in the presence of jamming," in *Military Communications Conference, 2008. (MILCOM 2008)*, vol., no., pp.1-7, 16-19 Nov. 2008, San Diego, CA, USA.

[33] W. Wenkai, L. Husheng, S. Yan, and H. Zhu, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *43rd Annual Conference on Information Sciences and Systems (CISS 2009)*, vol., no., pp.130-134, 18-20 March 2009, Baltimore, MD, USA.

[34] R. Chen; Jung-Min PlacePark; Y.T. Hou, and J.H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol.46, no.4, pp.50-55, April 2008.

[35] R. Chen, J.M. Park, and J.H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE J. Sel. Areas Commun.*, vol.26, no.1, pp.25-37, Jan. 2008.

[36] T.C. Clancy and K A. Hawar, "Security threats to signal classifiers using self-organizing maps," in *4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2009 (CROWNCOM 2009)*, vol., no., pp.1-6, 22-24 June 2009, Hannover, Germany.

[37] S. Anand, Z. Jin andd K.P. Subbalakshmi, "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks," in *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'08)*, vol., no., pp.1-6, 14-17 Oct. 2008, Chicago, IL, USA.

[38] W. Wang; H. Li; Y. Sun and Z. Han, "CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing," in *IEEE Global Telecommunications Conference (GLOBECOM 2009)*, vol., no., pp.1-6, Nov. 30 2009-Dec. 4, 2009, Honolulu, Hawaii, USA.

[39] R. Chen, J, M, Park, and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," in. *The 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, vol., no., pp.1876-1884, 13-18 April 2008, Phoenix, AZ, USA.

[40] F. Hu, S. Wang and Z. Cheng, "Secure cooperative spectrum sensing for Cognitive Radio networks," in *IEEE Military Communications Conference (MILCOM 2009)*, vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, USA.

[41] G.A. Safdar and M. O'Neill, "Common Control Channel Security Framework for Cognitive Radio Networks," in *69th IEEE Vehicular Technology Conference, (VTC Spring 2009)*, vol., no., pp.1-5, 26-29 April 2009, Barcelona, Spain.

[42] L. Husheng and H. Zhu, "Catching Attacker(s) for Collaborative Spectrum Sensing in Cognitive Radio Systems: An Abnormality Detection Approach," in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2010)*, vol., no., pp.1-12, 6-9 April 2010, Singapore.

[43] N.R. Prasad, "Secure Cognitive Networks," in *European Conference on Wireless Technology (EuWiT 2008)*, vol., no., pp.107-110, 27-28 Oct. 2008, Amsterdam, The Netherlands.

[44] A. N. Mody, R. Reddy, T. Kiernan, and T.X. Brown, "Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard," in *IEEE Military Communications Conference (MILCOM 2009)*, vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, USA.

[45] W. Wenkai, L. Husheng, S. Yan and H. Zhu, "Securing Collaborative Spectrum Sensing against Untrustworthy Secondary Users in Cognitive Radio Networks", *Eurasip Journal on Advances in Signal Processing*, *special issue on Advanced Signal Processing for Cognitive Radio Networks, vol. 2010*, Article ID 695750, 15 pages, 2010.

[46] L. Zhu and Z. Huaibei, "Two Types of Attacks against Cognitive Radio Network MAC Protocols," in *2008 International Conference on Computer Science and Software Engineering (CSSE 2008),* , vol.4, no., pp.1110-1113, 12-14 Dec. 2008, Wuhan, Hubei, China.

[47] A. Brawerman, D. Blough and B. Bing, 2004, "Securing the download of radio configuration files for software defined radio devices", in *Proc. of the second international workshop on Mobility management & wireless access protocols (MobiWac 2004)*. ACM, New York, NY, USA.

[48] H. Uchikawa, K. Umebayashi, and R. Kohn, "Secure download system based on software defined radio composed of FPGAs," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2002)*, vol.1, no., pp. 437- 441 vol.1, 15-18 Sept. 2002, Lisboa, Portugal.

[49] J. CityHoffmeyer, StateIl-PlaceNamePyung PlaceTypePark, M. Majmundar, and S. Blust, "Radio software download for commercial wireless reconfigurable devices," *IEEE Commun. Mag.*, vol. 42, no.3, pp. S26- S32, Mar 2004.

[50] H. Shiba, K. Uehara and K. Araki, "Proposal and evaluation of security schemes for software-defined radio," in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2003)*, vol. 1, 2003, pp. 114–118, Beijing, China.

[51] E. Gallery and C. Mitchell, "Trusted computing technologies and their use in the provision of high assurance SDR platforms," in *2006 Software Defined Radio Technical Conf. Product Exposition*, Nov 2006, Orlando, Florida, USA.

[52] J. Alves-Foss, P. W. Oman, C. Taylor, and W. S. Harrison, "The MILS architecture for high-assurance embedded systems," *International J. Embedded Syst.*, vol. 2, no. 3/4, pp. 239–247, 2006.

[53] J. Alves-Foss, C. Taylor, and P. Oman, "A multi-layered approach to security in high assurance systems," in *Proc. 37th Annual Hawaii International Conf. Syst. Sciences (HICSS 2004) - Track 9, 2004.*, vol. 9, Jan. 2004, Big Island, HI, USA.

[54] D. Murotake and A. Martin, "Updated system threat analysis for high assurance software defined radios", in *Proceedings, SDR'05 Technical Conference, SDR Forum*, Anaheim, CA, November 2005.

[55] Z. Kun, P. Paweczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters,* vol.14, no.3, pp.226-228, March 2010.

[56] L. Duan, Z. Lei, C. Yujun, and L. Shouyin, "Cooperative Spectrum Sensing with Double Threshold Detection Based on Reputation in Cognitive Radio," in *5th International Conference on Wireless Communications, Networking and Mobile Computing, (WiCom 2009)*, vol., no., pp.1-4, 24-26 Sept. 2009, Beijing, China.

[57] W. Wenkai, L. Husheng, S. Yan, and H. Zhu, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *43rd Annual Conference on Information Sciences and Systems (CISS 2009)* , vol., no., pp.130-134, 18-20 March 2009, Baltimore, MD, USA.

[58] P. Kaligineedi, M. Khabbazian and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio system," in *IEEE International Conference on Communications (ICC 2008)*, vol., no., pp.3406-3410, 19-23 May 2008, Beijing, China.

[59] Y. Peng, X. FengHong, L. Hua, and P. Jie, "The Research of Cross-Layer Architecture Design and Security for Cognitive Radio Network," in *International Symposium on Information Engineering and Electronic Commerce (IEEC 2009).*, vol., no., pp.603-607, 16-17 May 2009. Ternopil, Ukraine.

[60] P. Anand, A.S. Rawat, C. Hao, and P.K. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in Cognitive Radio Networks," in *Second International Conference on Communication Systems and Networks (COMSNETS 2010),*, vol., no., pp.1-9, 5-9 Jan. 2010, Bangalore, India.

[61] X. Shaoyi, S. Yanlei, and W. Haiming, "Double Thresholds Based Cooperative Spectrum Sensing Against Untrusted Secondary Users in Cognitive Radio Networks," in *IEEE 69th Vehicular Technology Conference, (VTC Spring 2009)*, vol., no., pp.1-5, 26-29 April 2009, Barcelona, Spain.

[62] F.R. Yu, H. Tang, H. Minyi, L. Zhiqiang, and P.C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *IEEE Military Communications Conference, (MILCOM 2009),* vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, USA.

[63] T. Yucek, H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surveys Tutorials*, vol.11, no.1, pp.116-130, First Quarter 2009.

[64] R. Chen, J.M. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, (SDR 2006)*, vol., no., pp.110-119, 25-25 Sept. 2006, Orlando, Florida, USA.

[65] Z. Tingting, Z. Yuping, "A New Cooperative Detection Technique with Malicious User Suppression," *IEEE International Conference on Communications, (ICC 2009)*, vol., no., pp.1-5, 14-18 June 2009, Dresden, Germany.

[66] Y. Zhao, J. H. Reed, S. Mao, and K. K. Bae, "Overhead Analysis for Radio Environment Map-enabled Cognitive Radio Networks," *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, (SDR 2006),* vol., no., pp.18-25, 25-25 Sept. 2006, Orlando, Florida.

[67] Caidan Zhao; Liang Xie; Xueyuan Jiang; Lianfen Huang; Yan Yao; , "A PHY-layer Authentication Approach for Transmitter Identification in Cognitive Radio Networks," *2010 International Conference on Communications and Mobile Computing (CMC 2010),* vol.2, no., pp.154-158, 12-14 April 2010, Shenzhen, China.

[68] O.R. Afolabi, K. Kiseon, Ahmad, A, "On Secure Spectrum Sensing in Cognitive Radio Networks Using Emitters Electromagnetic Signature," *Proc. of 18th International Conference on Computer Communications and Networks, (ICCCN 2009)*, vol., no., pp.1-5, 3-6 Aug. 2009, San Francisco, CA, USA.

[69] M. Kuroda, R. Nomura, W. Trappe, "A Radio-independent Authentication Protocol (EAP-CRP) for Networks of Cognitive Radios," *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON 2007)*, vol., no., pp.70-79, 18-21 June 2007, San Diego, California, USA.

[70] M. CityLima, A. dos Santos, G. Pujolle, "A survey of survivability in mobile ad hoc networks," *IEEE Commun. Surveys Tutorials*, vol.11, no.1, pp.66-77, First Quarter 2009.

[71] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public key management for mobile ad hoc networks. *IEEE Trans. Mobile Comput.*, Vol. 2, No. 1, pp. 52–64, 2003.

[72] G. Jakimoski and K.P. Subbalakshmi, "Towards Secure Spectrum Decision," *IEEE International Conference on Communications, (ICC 2009)*, vol., no., pp.1-5, 14-18 June 2009, Dresden, Germany.

[73] G.A. Safdar and M. O'Neill, "Common Control Channel Security Framework for Cognitive Radio Networks," in the *69^{th} Vehicular Technology Conference (VTC Spring 2009),* vol., no., pp.1-5, 26-29 April 2009, Barcelona, Spain.

[74] Y. Guosen, W. Xiaodong and M. Madihian, "Design of Anti-Jamming Coding for Cognitive Radio," in *IEEE Global Telecommunications Conference, (GLOBECOM 2007)*, vol., no., pp.4190-4194, 26-30 Nov. 2007, Washington D.C., USA.

[75] Y. Guosen and W. Xiaodong, "Anti-jamming coding techniques with application to cognitive radio," *IEEE Trans. Wireless Commun.,* , vol.8, no.12, pp.5996-6007, December 2009.

[76] F. Meucci, S.A. Wardana and N.R. Prasad, "Secure Physical Layer using Dynamic Permutations in Cognitive OFDMA Systems," in *IEEE 69th Vehicular Technology Conference, (VTC Spring 2009)*, vol., no., pp.1-5, 26-29 April 2009.

[77] G. Atia, A. Sahai, and V. Saligrama, "Spectrum enforcement and liability assignment in cognitive radio systems," in *Proc. of the Third IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DYSPAN 2008)*, Oct. 2008, Chicago, IL.

[78] F.R. Yu, H. Tang, H. Minyi, L. Zhiqiang and P.C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in *IEEE Military Communications Conference, (MILCOM 2009)*, vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, 2009.

[79] J. Giacomoni and D.C. Sicker, "Difficulties in providing certification and assurance for software defined radios," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN 2005).*, vol., no., pp.526-538, 8-11 Nov. 2005.

[80] S. Nagel, V. Blaschke, J. Elsner, F. K. Jondral, and D. Symeonidis, "Certification of SDRs in new public and governmental security systems," in *SDR Technical Conf. Product Exposition (SDR 2008)*, Oct. 2008.

[81] Federal Communications Commission, "In the matter of facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, report and order," Mar. 2005, FCC 05-57, ET Docket No. 03-108.

[82] FP7 EULER CORDIS web page. http://cordis.europa.eu. Last accessed 27/06/2010.

[83] D. Symeonidis and G. Baldini, "European Standardization and SDR Certification," in *Telecommunications (AICT), 2010 Sixth Advanced International Conference on*, vol., no., pp.136-141, 9-15 May 2010, Barcelona, Spain.

[84] A.R. Biswas, T.C. Aysal, S. Kandeepan, D. Kliazovich and R. Piesiewicz, "Cooperative Shared Spectrum Sensing for Dynamic Cognitive Radio Networks," in *IEEE International Conference on Communications, (ICC 2009)*, vol., no., pp.1-5, 14-18 June 2009, Dresden, Germany.

[85] W. Xu, P. Kamat, and W. Trappe, "TRIESTE: A Trusted Radio Infrastructure for Enforcing SpecTrum Etiquettes," in *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, (SDR 2006)*, vol., no., pp.101-109, 25-25 Sept. 2006.

[86] L. Xiaohua, C. Jinying, and N. Fan, "Secure transmission power of cognitive radios for dynamic spectrum access applications," in *42nd Annual Conference on Information Sciences and Systems, (CISS 2008)*, vol., no., pp.213-218, 19-21 March 2008.

[87] Common Criteria, National Institute of Standards and Technology Std. [Online]. Available: http://csrc.nist.gov/cc/.

[88] Wireless Innovation Forum's Security Working Group. Securing Software Reconfigurable Communications Devices. Document Id: WINNF-08-P-0013.

[89] D. Borth, R. Ekl, B. Oberlies, and S. Overby, "Considerations for Successful Cognitive Radio Systems in US TV White Space," in *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN 2008),* vol., no., pp.1-5, 14-17 Oct. 2008.

[90] C. Stevenson, G. Chouinard, L. Zhongding, H. Wendong, S. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol.47, no.1, pp.130-138, January 2009.

[91] EEE 802.22 Draft Standard, on Wireless Regional Area Networks ("WRANs"), for a cognitive radio-based PHY/MAC/air interface. http://grouper.ieee.org/groups/802/22/.

[92] N. Chetan and K.P. Subbalakshmi, "Security Issues in Cognitive Networks", Book Chapter in *Cognitive Networks: Towards Self-Aware Networks*, Ed. Qusay H. Mahmoud, Wiley, pp: 271-292, ISBN: 978-0-470-06196-1, 2007.

[93] A. Mody, R. Reddy, M Sherman, T. Kiernan, and D. J. Shyy, "Security and Protocol Reference Model Enhancements in IEEE 802.22," https://mentor.ieee.org/802.22/dcn/08/22-08-0083-08-0000security-and-prm-enhancements-in-80222-v3.ppt.

[94] E.O. Nuallain, "A Proposed Propagation-Based Methodology with Which to Address the Hidden Node Problem and Security/Reliability Issues in Cognitive Radio," in *4th International Conference on Wireless Communications, Networking and Mobile Computing, (WiCOM 2008)*, vol., no., pp.1-5, 12-14 Oct. 2008.

[95] D.W. Bliss, "Optimal SISO and MIMO Spectral Efficiency to Minimize Hidden-Node Network Interference," *IEEE Commun. Lett.*, vol.14, no.7, pp.620-622, July 2010.

[96] F. Granelli, P. Pawelczak, R.V. Prasad, K.P. Subbalakshmi, R. Chandramouli, J.A. Hoffmeyer, and H.S. Berger, "Standardization and research in cognitive and dynamic spectrum access networks: IEEE SCC41 efforts and other activities," *IEEE Commun. Mag.*, vol.48, no.1, pp.71-79, January 2010.

[97] D. Gozupek, S. Bayhan, and F. Alagoz, "A novel handover protocol to prevent hidden node problem in satellite assisted cognitive radio networks," in *3rd International Symposium on Wireless Pervasive Computing*, *(ISWPC 2008)*, vol., no., pp.693-696, 7-9 May 2008.

[98] A. De Domenico, E. Calvanese Strinati, and M.G. Di Benedetto, "A Survey on MAC Strategies for Cognitive Radio Networks," *IEEE Commun. Surveys Tutorials*, vol.PP, no.99, pp.1-24, 0

[99] T. Clancy, and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation", in *Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, May 2008.

[100] F. Perich, and M. McHenry, "Policy-based spectrum access control for dynamic spectrum access network radios", in *Web Semantics: Science, Services and Agents on the World Wide Web*, Volume 7, Issue 1, The Semantic Web and Policy, January 2009, Pages 21-27, ISSN 1570-8268.

Gianmarco Baldini completed his degree in 1993 in Electronic Engineering from the University of Rome "La Sapienza" with specialization in Wireless Communications. He has worked as Senior Technical Architect and System Engineering Manager in Ericsson, Lucent Technologies, Hughes Network Systems and Selex Communications before joining the Joint Research Centre of the European Commission in 2007 as Scientific Officer. His current research activities focus on communication services for Public Safety, security aspects in GNSS services and modeling of critical infrastructures.

Dr. Michael Street is Principal Scientist-Communication Systems at the Chief Technology Office, NATO C3 Agency. He began writing software radios in 1992 during a PhD studying adaptive behavior for HF radio networks. He has since worked in academe, industry and government, joining NC3A in 1999 and leading NATO work on SDR, security and spectrum use at NC3A since 2004.

Dr. Abdur Rahim Biswas has completed his Bachelor degree from Bangladesh, Master degree from Sweden and PhD from Germany. He is a technical leader of "Cognitive UWB radio and Coexistence" work group in FP7 EUWB project. He has several contributions in European cognitive radio standardization body ETSI TC RRS (Reconfigurable Radio System). He is also leader of Spectrum Enablers Group (SEG) within European Commission (EC) concentration Radio Access and Spectrum (RAS) cluster. At present, he is a senior research staff in CREATE-NET, ITALY. He has several years experience in cognitive radio and coexistence, interference mitigation techniques, security, standardization and regulation, etc. He is also the steering committee member of CROWNCOM (International Conference on Cognitive Radio Oriented Wireless Networks and Communications).

Dr. Taj A. Sturman MEng MPhil PhD CEng MIET MIEEE. Taj is an experienced systems engineer with a strong background in military communications, with over fifteen year's experience, presently employed at EADS Astrium (Portsmouth, UK) as a Senior Communication Systems Engineer. He has been engaged in modelling, analysing and evaluating various aspects of communication systems and networks. He participates in various Security and Interoperability Activities at both the European and International Level; examples of which include EULER project, Waveform Design and Diversity Conferences for both IET and IEEE, and Studies for Ofcom. Prior to his employment, Taj gained a PhD, MPhil(Q) and an MEng(Hons) degree all in Electronic and Electrical Engineering at the University of Birmingham (UK) investigating Secure Communications.

Dr. Ruediger Leschhorn is the Head of Studies in the Radio Communication Systems Division of Rohde & Schwarz. He received the diploma degree in electrical engineering in 1980 from the Technical University of Munich, Germany and the doctoral degree in 1987 from the University of the German Armed Forces, where he worked in the area of microwaves. Ruediger Leschhorn is active in various working groups and forums, among others in the Wireless Innovation Forum (former SDR Forum), where he currently is the Vice Chair of the Forum and the Chair or the SCA Test & Evaluation Work Group.

Gyözö Gódor received his M.Sc. degree in electrical engineering, from Budapest University of Technology and Economics (BUTE), Budapest, Hungary, in 2003. He is currently a Ph.D. candidate and he is an assistant professor at the Department of Telecommunications of BUTE. He is a member of Mobile Communications and Computing Laboratory (MC2L), an associate member of the IEEE, IEEE Communications Society. His research interests include mobile and wireless network security and reliability, security issues and lightweight authentication protocols of heterogeneous and sensor networks, elliptic curve cryptography based authentication protocols for small computational capacity environment, and QoS support and medium access methods for wireless LANs.