Security in Cognitive Radio Networks

Kresimir Dabcevic, Lucio Marcenaro, Carlo S. Regazzoni
University of Genova, Italy

Please cite this document as:
MLA

APA

Chicago
Abstract

While bringing the potential for solving the spectrum underutilization problem using methods such as dynamic and opportunistic spectrum access, Cognitive Radios (CRs) also bring a set of security issues and potential breaches that have to be addressed. These issues come out mainly from the two important capabilities implemented within CRs: their cognition ability and reconfigurability.

This chapter will focus on identifying, presenting and classifying the main potential security attacks and vulnerabilities, as well as proposing appropriate counter-measures and solutions for them.

These will be supplemented by simulation results and metrics, with the intention of estimating the efficiency of each of the observed attacks and its counter-measure. The presented simulations are performed in the proprietary C/C++ and Matlab/Simulink simulators.

nSHIELD is a major ongoing European embedded systems security-related project, which will be used to demonstrate the practicability of the potential implementation of the proposed countermeasures and solutions for the discussed security problems and issues.
INTRODUCTION

With the continuous market penetration of many spectrum-demanding radio-based services, such as video broadcasting, finding ways to increase the spectrum usage efficiency has become a necessity. Cognitive Radio (CR) is a technological breakthrough that – by utilizing concepts such as Opportunistic Spectrum Access (OSA) and Dynamic Spectrum Access (DSA) – is expected to be an enabler for these improvements, making it a current “hot topic” within the radio-communication research community.

Cognitive radio can be described as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters as a response to the changes in the surrounding environment. Namely, its parameters can be reconfigured in order to accommodate the current needs of either the network operator, spectrum lessor, or the end-user.

Although this doesn’t necessarily need to be the case, Cognitive Radio (CR) is usually being defined as an upgraded and enhanced Software Defined Radio (SDR). Typically, full Cognitive Radios will have learning mechanisms based on some of the deployed machine learning techniques, and may potentially also be equipped with smart antennas, geolocation capabilities, biometrical identification, etc.

However, the newly-introduced cognitive capabilities are exactly what make Cognitive Radios susceptible to a whole new set of possible security issues and breaches. Furthermore, the threats characteristic to Software Defined Radios, as well as those characteristic to “traditional” wireless networks also need to be taken into account.

Cognitive Radio Network can be described as a network in which one or more users are Cognitive Radios. With the assumption of the potential attacker, as well as legitimate Secondary Users (SUs) always being CRs, the taxonomy of the threats within CRNs can be done with respect to the type of the Primary Users (PUs) considered, i.e.:

- PUs as “traditional” wireless systems,
- PUs as Software Defined Radios,
- PUs as Cognitive Radios.

It is worth noting that the proposed taxonomy is merely one of the possible approaches - the categorization can be done in several different ways. We have opted in for this particular approach because of its clarity and since it optimally fits the CR security framework that we are proposing in the last subsection.

The following subsection defines the basic concepts and premises of cognitive radios, and gives an introductory classification and basic definitions of CR-related threats. Section 3 will deal with the security of traditional wireless systems, describing legacy methods for protecting wireless communications such as WEP, WPA and WPA2, as well as the general security issues in wireless cellular networks. Section 4 highlights the security issues related to Software Defined
Radio systems, while Section 5 considers potential threats to Cognitive Radios. Results are shown for so-called Primary User Emulation Attacks and Smart Jamming Attacks.
BACKGROUND

One of the most important capacities of future Cognitive Radio systems is their capability to optimally adapt their operating parameters based on the observations and previous experience. There are several possible approaches towards realizing such cognitive capabilities, such as:

- Reinforcement learning,
- Learning based on neural networks,
- Game-theoretic approach.

Reinforcement learning refers to the machine learning method where radio learns through trial-and-error interactions in a scenario without perfect contextual information. It is a kind of mathematical method used for the learning state in the cognition cycle, which will learn the information (recorded in the form of weighting factors) based on the external environment and previous states, which then influence the current activation. The weight is used to show the influence from the previous users or the factors based on circumstance, which will be updated on each activation (Hu, 2011).

Artificial neural networks (ANN) are mathematical models inspired by the structure and functioning of biological neural networks (Bishop, 1995). ANNs can change and adapt their structure based on data used during a learning phase and are able to discover and model complex relationships among acquired data. ANN can be trained by automatically selecting one model from the set of allowed models for the network and this is typically done by minimizing a cost criterion. There are numerous algorithms available for training neural network models; most of them can be viewed as a straightforward application of optimization theory and statistical estimation. Most of the algorithms used in training artificial neural networks employ some form of gradient descent. This is done by simply taking the derivative of the cost function with respect to the network parameters and then changing those parameters in a gradient-related direction. Evolutionary methods (Ilonen, Kamarainen, & Lampinen, 2003), simulated annealing (Kirkpatrick, Gelatt, & Vecchi, 1983), expectation-maximization, non-parametric methods and particle swarm optimization (Kennedy & Eberhart, 1995) are some commonly used methods for training neural networks.

Game theory is a mathematical study of strategic interaction processes between multiple independent decision makers. Since within Cognitive Radio Networks, users can be modeled as such decision makers, the game theory presents itself as a natural structure for analyzing users’ behaviors and actions, as well as for modeling the suitable strategies in order to overcome the crucial interoperability issues between the cognitive users. Application of game theory to CRNs is multifold, ranging from ensuring a formalized approach for the dynamic spectrum sharing (DSS) related issues, through supplying different optimality criteria for the spectrum sharing, to deriving efficient distributed approaches for DSS by using the so-called non-cooperative game theory. Simpler game-theoretical solutions typically do not account for the learning capabilities of CRs, however it is possible to model more advanced games, such as Bayesian games, for dealing with algorithms with learning capabilities. Game theory can furthermore be viewed as an individual set of tools for analyzing the security-related issues, and has been studied e.g. in (Liu & Wang, 2011).
As stated, deployment of learning techniques represents one of the fundamental parts of the CR paradigm. By using one of the described approaches, CRs are able to observe and learn the status of the surrounding environment, which has an important application from the perspective of utilizing RF spectrum in a more efficient manner. The outcome of this learning process is used by the CR-enabled devices to improve the efficiency in accessing the available spectrum resources: CRs can, for example, learn different patterns of PUs’ activities in order to be able to forecast the availability of the resource and to adapt dynamically to the sensed conditions. The knowledge about the spectrum usage can be built by each individual unlicensed user without interaction with other users. Alternatively, the unlicensed users can collaborate in order to not only to exchange network information, but also to model and update the radio environments and typical activity patterns.

Deployment of these learning techniques, however, brings new potential weaknesses from the network security point of view. If a malicious user is aware of the learning capabilities of the CR devices in the network, it can adopt a specific activity pattern in order only to deceive the cognitive users, thus possibly dramatically decreasing the CRs’ and the network’s overall performance.

Whereas it is intuitive that each of the approaches for realization of the intelligent behavior within CRNs could suffer from their own potential vulnerabilities, these will not be considered separately. Instead, the main focus of the chapter will be on the vulnerabilities stemming out from the case where intelligent behavior within CRNs has been established, regardless of which approach was taken towards achieving it. The Objective Function Attack, described in the subsection “Other attacks and threats”, is an example of the direct attack on CR’s learning mechanism.

Security of traditional wireless systems is a well-studied topic, and a number of well-defined wireless security protocols are established and used nowadays. In cases where Primary Users within a CRN have only the properties and capabilities of the “traditional” (as opposed to Software Defined) digital transceivers, it is paramount to ensure the existence of such security measures and protocols.

Most widespread wireless security standards are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access version 2 (WPA2), which are presented in the following section, as well as the common security issues of the wireless cellular networks.

Since Cognitive Radios are by and large defined as upgraded and enhanced Software Defined Radios, it is important to establish which security threats are relevant for SDR networks, as well as which counter-measures need to be deployed.
SECURITY OF “TRADITIONAL” WIRELESS SYSTEMS

As has been stated, there are several established and commonly used security standards for wireless networks used today. In this chapter, the general security issues in cellular networks, as well as the most widespread mechanisms for the WLAN security – WEP, WPA and WPA2 – will be reviewed.

Security issues in wireless cellular networks

The openness of communication characteristic to the wireless cellular networks brings a set of security issues that need to be addressed. Being the standard that had the highest impact in the evolution of commercial wireless cellular networks, Global System for Mobile Communications (GSM) has throughout its existence been subjected to a particular attention from security standpoint.

GSM incorporates several built-in security features responsible for ensuring subscribers’ safety and privacy, namely (European Telecommunications Standards Institute, 1996):

- Authentication of the registered subscribers only,
- Secure data transfer through the use of encryption,
- Subscriber identity protection,
- Mobile phones are inoperable without a SIM,
- Duplicate SIM are not allowed on the network,
- Securely stored Ki.

Most of the security mechanisms in GSM are based on crypto algorithms, which vary depending on the functionality they are designed to protect. The main such algorithms are A5 – a stream cipher used for encryption, A3 – an authentication algorithm, and A8 – the key agreement algorithm. Among the initial two A5 algorithms, A5/1 is the stronger one, and is used to achieve security and privacy of voice over the air interface. Originally kept secret, it became publicly known after being reverse-engineered, and has continued to serve as a good example for crypto-related security hazards. A5/2 is the version without any export limitations, which after also being reverse-engineered and cryptanalyzed, showed the need for a more powerful algorithm. Hence, in 2002, A5/3 was introduced using the block-cipher called KASUMI. Besides GSM, KASUMI is used as a crypto algorithm in GPRS and 3G networks as well.

Authors in (Barkan, Biham, & Keller, 2008) have analyzed several attacks against A5 cyphers, namely:

- Class-Mark Attack - the attacker changes the class-mark information that the phone sends to the network at the beginning of the conversation, such that the network thinks that the phone supports only A5/2. Although the network prefers to use A5/1, it must use either A5/2 (or A5/0 — no encryption), as it believes that the phone does not support A5/1. The attacker can then listen in to the conversation through the cryptanalysis of the weaker A5/2 cipher.

- Recovering crypto key of past or future conversations - an attacker recovers the encryption key of an encrypted conversation that was recorded in the past.
• Man in the Middle Attack - The attacker uses a fake base-station in its communications with the mobile phone, and impersonates the mobile phone to the network, and forwards to the victim the authentication request that it got from the network. The victim sends the 32-bit Signed Response to the attacker, who holds on to it and, by performing a ciphertext attack finds the cipher key, and is able to authenticate himself on the network.

General Packet Radio Service (GPRS) is a protocol that enables the packet radio access for GSM users. From a security viewpoint, GPRS inherits many security problems from GSM, however the upgraded network architecture also brings several new ones. Author in (Xenakis, 2008) has evaluated the security aspects of the GPRS architecture, identifying the following weaknesses:

• Compromise of the confidentiality of subscriber identity - whenever the serving network cannot associate the Temporary Mobile Subscriber Identity (TMSI) with the International Mobile Subscriber Identity (IMSI), the Service GPRS Support Node (SGSN) should request the MS to identify itself by means of IMSI on the radio path. This leaves the possibility of modeling the attacker pretending to be a new serving network, to which the user has to reveal his permanent identity.

• One-way subscriber authentication - does not assure that a mobile user is connected to an authentic serving network, thus enabling active attacks using a false BS identity. Furthermore, the A3 and A8 vulnerabilities are inherited from the GSM network, whereas re-using authentication triplets makes it possible to launch Man in the Middle Attack, or Replay Attack.

• Encryption of signalling and user data is optional – leading to attacker being able to mediate in the exchange of authentication messages between the legitimate user and the BS.

• Unsupported security protection by the SS7 technology – this deficiency of the SS7 technology, which is used for signaling exchange in GPRS, increases the probability of an adversary to get access to the network or a legitimate operator to act maliciously as well as resulting in the unprotected exchange of signaling messages between the location registers.

Compared to its 2G and 2.5G predecessors, 3G has brought significantly better security features, mainly through the usage of the aforementioned KASUMI block cipher instead of the A5 stream cipher, and the Authentication and Key Agreement (AKA) protocol instead of CAVE-based authentication. Furthermore, 3G integrity algorithm with an Integrity Key (IK) introduces the feature of Data Integrity, whereas User to User Services Integrity Module (USIM) and USIM to Terminal Authentication provide the secure access to MS.

Long Term Evolution’s (LTE) security is largely built upon the 3G one (usage of the AKA protocol in the first place), with several modifications, such as extended key hierarchy, introduction of longer keys, better backhaul protection and integrated interworking security for legacy and non-3GPP networks.

Wired Equivalent Privacy
Wired Equivalent Privacy (WEP) was “designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication” (Lashkari, Danesh, & Samadi, 2009). It is an “optional encryption standard, implemented in the MAC layers, intended to provide user authentication, data privacy and data integrity in a manner that would make a wireless LAN equivalent to a wired LAN” (Borse & Shinde, 2005).

The RC4 algorithm – also known as a stream cipher – is a symmetric cipher in which every binary digit in a data stream is subjected separately to encrypting algorithm, by logically XOR-ing the key to the data. The key is shared between communicating nodes, clients and access points, and ensuring its secure exchange is needed.

One of the main vulnerabilities of the WEP protocol lies in the usage of the random Initialization Vector (IV), used in the encryption process. Namely, WEP’s IV is only 24 bit long, allowing for a number of unique combinations that can be reached fairly easily in busy network conditions, bringing the need for the re-use of certain IVs. Hence, if RC4 for a certain IV is found, potential attacker can decrypt the packets with the same IV.

Furthermore, WEP does not define a key management protocol, leading to the need for manual change of the key for each wireless device by the network administrator. This presents a big security leak, since in case of a potential security breach all keys need to be changed, which – due to the lack of synchronization - is far from a trivial task.

The use of the RC4 also brings an issue of weak keys – the high correlation factor between the key and the output means that the attacker can somewhat easily filter out the “interesting packets”, substantially decreasing the number of combinations for possible keys that will allow him the access to the network.

There are two forms of authentication within 802.11 standards: Shared key and Open system. And while the latter one gives a more satisfactory performance in terms of security, the Shared key authentication – based on encryption of a challenge – brings a potential security breach in cases where attackers are able to monitor the encryption process.

Authors in (Borisov, Goldberg, & Wagner, 2001) define four basic types of attacks present in WEP-based wireless networks:

- **Passive Attack** - a passive eavesdropper can intercept all wireless traffic, until an IV collision occurs. Once the attacker obtains the XOR of the two plaintext messages, the resulting XOR can be used to infer data about the contents of the two messages. IP traffic is often very predictable and includes a lot of redundancy, which can be used to eliminate many possibilities for the contents of messages.

- **Active Attack to Inject Traffic** – if the attacker knows the exact plaintext for one encrypted message, he can use this knowledge to construct correct encrypted packets. The procedure involves constructing a new message, calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the new message.

- **Active Attack from Both Ends** - the attacker makes a guess about the headers of a packet, which is usually easy to obtain or guess. The attacker can flip appropriate bits to transform the destination IP address to send the packet to a machine he controls, and transmit it using a rogue mobile station. Most wireless installations have Internet connectivity; the packet will be successfully decrypted by the access point and forwarded...
unencrypted through appropriate gateways and routers to the attacker's machine, revealing the plaintext.

- **Table-based Attack** - the small space of possible initialization vectors allows an attacker to build a decryption table. Once he learns the plaintext for some packet, he can compute the RC4 key stream generated by the IV used, which can then be used to decrypt all other packets that use the same IV. Over time, the attacker can build up a table of IVs and corresponding key streams.

**Wi-Fi Protected Access**

Wi-Fi Protected Access (WPA) is an open standard aimed at solving problems present in WEP-based systems. Encryption is realized through the Temporal Key Integrity Protocol (TKIP), which provides per-packet key mixing function for reducing correlation between IVs from weak keys. Also, message integrity check, as well as the re-keying mechanism is added. RC4 is also used within TKIP, with an addition of hashing, making for a significantly more robust mechanism.

Authors in (Lashkari, Danesh, & Samadi, 2009) break down the improvements that WPA brings over WEP as:

- A cryptographic message integrity code, or MIC, to defeat forgeries,
- A new IV sequencing discipline, to remove replay attacks from the attacker’s arsenal,
- A per-packet key mixing function, to de-correlate the public IVs from weak keys,
- A re-keying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

For home networks, a so-called WPA Pre-Shared Key (WPA-PSK) variation has been designed. It is a simplified algorithm, in which individual user must set a passphrase (key). Difference with WEP lies in automatic alteration of the key every \( n \) time intervals, making it more difficult for attackers to identify them. However, WPA-PSK algorithm has proven to be more attack-prone. Several dictionary attacks were devised to somewhat efficiently exploit the Pairwise Master Key (PMK) – a feature obtained from the concatenation of the passphrase, Service Set Identifier (SSID), its length, and a number of bit strings used in a session.

**Wi-Fi Protected Access version 2**

Wi-Fi Protected Access 2 (WPA2), also known as the 802.11i, is an amendment to the WPA standard, aiming at improving not only security and reliability, but also the ease of access of the WPA-based networks.
Security in Cognitive Radio Networks

One of the most important novelties is the introduction of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). It is based on Advanced Encryption Standard (AES) – an open-source algorithm that provides significant robustness improvements. As is the case with WPA, the most exploitable vulnerability of WPA2 stems out from using the PSK key.

In WPA2, user authentication is separated from ensuring the privacy and integrity of the messages, and, like WPA, it operates in two modes:

- **WPA-Personal** – or Pre-Shared Key (PSK) – performed between the client and the access point, and typical for home networks,
- **WPA-Enterprise** – or Extensible Authentication Protocol (EAP) – typical for business networks. Authentication server named RADIUS is used for authorization decisions - it provides the Master Session Key to the client and the access point.

Up to date, WPA2 is considered the most reliable Wi-Fi security protocol, however few vulnerabilities are still present.

Authors in (Dengg, Friedl, Hörtl, Jäger, Lehner, & Macskási, -) recognize the following attacks on WPA2-secured systems:

- **PSK Brute Force Dictionary Attack** – based on attacking the PSK, recognized as WPA2’s biggest weakness. To perform an attack on the pass-phrase the attacker must eavesdrop the network during the 4-way handshake in phase 4 for the PTK, where he receives all but the pass-phrase, and then perform the attack.
- **Security Level Rollback Attack** – based on WPA2’s feature of defining a TSN (Transient Security Network). The attacker sends wrong Beacon or Probe requests to establish a Pre-RSNA connection, even if both would support a more secure RSNA connection like WPA2. As Pre-RSNA does not support a cipher suite, they won't be able to detect the fraud and accept the insecure connection. The attacker is now able to get the default keys by exploiting WEP's weaknesses.
- **Reflection Attack** – present in ad-hoc networks, where a device is not allowed to play both the supplicant and authenticator roles at the same time. The original device starts the handshake as authenticator, the attacker starts another 4-way handshake using the same parameters but the device as supplicant. Once the device starts to send messages as supplicant, the attacker can use these messages as a valid message for the initial 4-way-handshake of the attacker’s target.

In addition to those, (AirTightNetworks, 2012) recognize the so-called “Hole196” vulnerability, which exposes WPA2-secured network to insider attacks. The attack is enabled by the usage of the group temporal key (GTK), shared among all authorized clients in a WPA2 network. The data traffic encrypted using the GTK should be transceived between an access point and a legitimate user, however a malicious inside user can potentially eavesdrop and decrypt data from other authorized users as well as scan their Wi-Fi devices for vulnerabilities, install malware and possibly compromise those devices.

Wi-Fi Alliance continuously works on improving the WPA and WPA2 standards, offering different EAP types, allowing for greater interoperability and higher security. Nevertheless, certain security issues still exist, and improvements still need to be made.
In future Cognitive Radio Networks, it is feasible to expect the presence of non-CR and non-SDR wireless terminals, i.e. the systems that are commonly deployed today. But also, the wireless nature of SDRs and CRs points to the fact that such systems will also be prone to inheriting the threats present to the aforementioned, “traditional” systems. Hence, ensuring maximum security and privacy of such systems will be paramount, and addressing the known security issues in the current state-of-the-art security standard – WEP2 – can be considered a good starting point.
SECURITY OF SOFTWARE DEFINED RADIOS

There is no unanimous definition of what requirements a radio must satisfy in order to be considered software defined. One of the most recognizable, and in the same time very intuitive ones is Wireless Innovation Forum’s one, which recognizes SDR as “a radio in which some or all of the physical layer functions are software defined” (Wireless Innovation Forum). These functions usually include - but are not limited to – frequency, modulation technique, cryptography, used bandwidth, coding technique, etc. However, the level of reconfigurability/reprogrammability needed for the radio to be labeled as an SDR isn’t strictly defined.

Hence, depending on this level of software reconfigurability, different authors establish a division between, for example, Software Capable, Software Programmable and Software Defined Radios.

For the sake of the simplicity, all of these will from now on be marked as Software Defined Radios, as from the security point of view, they mostly share common threats and problems.

For the future purposes, it is useful to categorize the types of software present in Software Defined Radios, as per Wireless Innovation Forum’s guidelines, since this categorization is widely accepted in the scientific environment, and is commonly referred to.

Following that, it is possible to classify the software in SDRs as:

- Radio Operating Environment (ROE) - consists of the core framework, the operating system, device drivers, middleware, installer and any other software fundamental to the operation of the radio platform,

- Radio Applications (RA) - software which controls the behavior of the RF function of the radio. This includes any software defining the air interface and the modulation and communication protocols, as well as software used to manage or control the radio in a network environment,

- Service provider applications (SPA) - software used to support network and other service provider support for the user of the radio. It includes voice telephone calls, data delivery, paging, instant messaging service, video pictures, emergency assistance, and geolocation,

- User applications (UA) - application software not falling into any of the above categories.

General SDR-related security threats

One of the potential hazards in SDRs lies in the possibility of tampering the hardware of SDRs. Since these hazards apply to all wireless systems and are not unique to the new features that SDRs bring, the focus will be on the other types of threats – the ones stemming out from the software reconfigurability. Main threats to the reconfigurability come from faulty and buggy software, so the deployed schemes need to protect the system from download and usage of the improper software.

In general, security-enabling mechanisms for SDRs can be divided into hardware-based and software-based ones, each with their own advantages and disadvantages.
Hardware-based mechanisms include hardware modules for monitoring the SDR’s reconfigurable parameters. However, unlike the SDRs they are securing, these mechanisms themselves are typically not easily reconfigurable, and updating the security parameters or policies may be problematic and expensive.

Software-based mechanisms rely on deploying the tamper-resistance techniques, providing safe and secure authentication, communication security and integrity, as well as safe algorithms for download, updating and distribution of the software. The potential vulnerability of such schemes is the openness to malicious modification.

In (Li, Raghunathan, & Jha, 2009), authors present a security architecture based on separation of the application environment and the radio operation environment, so that the compromise of one doesn’t affect the other. Furthermore, SDR reconfiguration parameters produced by the application environment are checked against security policies before they take effect in the radio environment. So, in cases where application environment is tampered with and becomes malicious, it cannot infect the radio environment and thus the RF characteristics can be ensured to be in compliance with the desired policies.

For software classification, the authors have used Wireless Innovation Forum’s guidelines, as was described before, where on top of the ROE, RA, and SPA they are defining the User Application Environment (UAE) as the environment (OS) where UA are executed. Authors define a new separate layer called secure radio middleware (SRM) – a layer implemented below UAE, which includes the most security-critical components, namely RA and ROE. SRM is composed of:

- Bypass – in charge of non-critical operations,
- Memory Management Unit – controls the behavior of the OS,
- Virtualized Hardware – where all the radio applications are performed,
- Security Policy Monitor – tries to decide a normal value or range for the radio parameters and compare them to the ones the OS passes to Virtualized Hardware, leading to initialization of the appropriate recovery mechanisms in cases of violation.

As the authors themselves note, their implementation has several constraints. Since a desktop PC has been used as a testbed, the implementation doesn’t reflect the performance in the potential real-life scenarios, where platforms will typically be far more resource-constrained. Furthermore, their architecture doesn’t incorporate mechanisms for encryption/decryption, information integrity, access control and secure radio software download, which are issues that need to be addressed separately.

Authors in (Brawerman, Blough, & Bing, 2004) propose the lightweight version of a Secure Socket Layer (SSL) protocol. SSL provides bulk encryption, end point authentication and data integrity protection. For encryption, symmetric key algorithms are used, whereas for authentication, client and server can mutually authenticate each other.

LSSL redesigns the SSL protocol in order to decrease the computational complexity of the performed operations and perform most of the cryptography at the server side, thus making it suitable for power-constrained devices, such as SDR terminals.

The authors have defined several possible attacks, and the corresponding defense feature employed within the protocol, namely:
Security in Cognitive Radio Networks

- Access control – countered by the authentication mechanism.
- Masquerade attack – attacker emulates the manufacturer server or a client, which protocol counters using mutual authentication.
- Confidentiality – secrecy of information is ensured by establishing secure connections.
- Replay – attacker re-transmits messages after a certain time period. Protocol tackles this by using timestamps.
- R-CFG validation – installation of the non-approved R-CFG, resolved by digitally signing every R-CFG by the regulatory agency.
- R-CFG integrity – possibility of modifying R-CFG after it has been approved, countered by using one-way hash functions.

Potential threats to common SDR architectures

Currently, there are two predominant open-source architectures for SDRs: GNU Radio – particularly appealing to academic environment due to the relative simplicity of use and compatibility with the low-cost off-the-shelf SDR platforms such as USRP, and Software Communications Architecture (SCA) – architecture adopted by the Wireless Innovation Forum.

GNU Radio is an open-source software toolkit that, coupled with hardware equipment such as USRP, allows for a complete platform for building Software Defined Radios (although GNU Radio can also be used as a stand-alone software package). Most of GNU Radio’s applications are written in Python, whereas C++ is used for implementing signal processing blocks. Python commands are used to control all of the USRP’s software defined parameters, such as transmit power, gain, frequency, antenna selection, etc. GNU Radio is built on two main structural entities – signal processing blocks and flow graphs. Blocks are structured to have a certain number of input and output ports, consisting of small signal-processing components. When the blocks are appropriately connected, a flow graph is made.

Authors in (Hill, Suvda, & Campbell, 2005) have analyzed threats related to GNU Radio-based SDR systems. They refer to the GNU Radio Software Applications – written in C++ – as to the Radio Applications (RA), and to the Python functions as to the Radio Operating Environment (ROE). As such, they identify the following shortcomings related to the ROE of GNU Radio:

- At the moment, there is no embedded functionality for verification, i.e. securing the SDR device from being reconfigured by the malicious code.
- Presence of the risks related to the execution of models in the graph – since a single address space is shared among all the software modules, there is a possibility for the malicious user to alter the data in the whole address space. To counter this, they propose restricting each module to only be able to access its dedicated address space.
- Possibility of a buffer overflow, coming out from the use of the shared buffer. Mechanisms for restricting the amount of data possibly written to the buffer are needed.
They also define three possible attacks, depending on the parameter targeted:

- Modulation attack – improper change of the modulation format,
- Frequency attack – jamming attacks where an impostor is transmitting on the frequencies that it’s not allowed to,
- Output power attack – where an attacker can continuously transmit at high power, forcing other users to increase their power level, which leads to increased battery drain.

Authors go on to suggest that GNU Radio ROE has to provide mechanisms for evaluating and enforcing policies for specifying the operating constraints of the SDRs, defined by the network administrators and regulators.

Software Communications was originally defined by the US government with the purpose of securing waveform portability and improving software reuse. Built originally for US military’s Joint Tactical Radio System (JTRS) program, it has been accepted as a communication standard in military services of many other countries, but also by commercial organizations such as Wireless Innovation Forum. It is an always-evolving standard - with first version dating from 2000 – that provides standardized set of methods for installing, managing and de-installing new waveforms, therefore maintaining interoperability of various SDR systems.

The Software Communications Architecture (SCA) is an open architecture framework that instructs the designers as to how the elements of hardware and software should operate in harmony within the JTRS. It governs the structure and operation of the JTRS, enabling programmable radios to load waveforms, run applications, and be networked into an integrated system. Design engineers use the Software Communications SCA definition document just as an architect or planner uses a local building code to design and build homes. Security is a very important aspect of radios featuring SCA. The architecture provides the foundation to solve issues like programmable cryptographic capability, certificate management, user identification and authentication, key management, and multiple independent levels of classification. Manufacturers and users are embracing the approach, albeit much more slowly than preferred. For example, the Security Supplement to the JTRS SCA requires that SDR devices “shall only accept cryptographic algorithms/algorithms packages signed by National Security Agency (NSA),” that “NSA shall digitally sign all Security Policy XML files,” and that “the operating system invocation method shall be a NSA digitally signed script”. However, SDR middleware and tools vendors supporting JTRS customers do not yet support digital signature features within their products, although they express openness to including such features in future releases. Similarly, user and manufacturer representatives in the SDR Forum’s Public Safety SIG are trying to identify alternatives to digital signatures before committing to such an approach, largely due to perceptions about public key infrastructure (PKI) technology complexity.
## SECURITY OF COGNITIVE RADIOS

As described before, cognitive radios can be considered as intelligent devices that are able to learn from the experience and dynamically adapt to the features of the environment. Major research efforts have been devoted towards the study and development of learning and reasoning techniques without considering security related issues in detail. Typically, security is tackled by means of adding authentication on encryption mechanism to the data communication within the network, but this is not always sufficient due to the improved capabilities of the cognitive paradigm. In particular, as artificial intelligence engines represent the core of cognitive devices, potential threats that are able to feed CRs with false sensory inputs – thus purposely affecting its trained knowledge and subsequently its behavior - should be considered.

The following table summarizes the attacks and the proposed defense mechanisms addressed in this section, also describing their basic characteristics:

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Contribution</th>
<th>Attacker’s special characteristics</th>
<th>Proposed defense scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUEA – emulating characteristics of a primary user to acquire exclusive spectrum rights</td>
<td>Chen, Park, &amp; Reed, 2008</td>
<td>Altering its transmit power, modulation mode and frequency; injecting false data to the localization system</td>
<td>3-step mechanism: verification of signal characteristics, RSS measurement, localization of the signal</td>
</tr>
<tr>
<td></td>
<td>Chen, Cooklev, Chen, &amp; Pomalaza-Raez, 2009</td>
<td>Applying the estimation techniques to enhance its performance</td>
<td>Assumes that emulating the channel features is not feasible for the attacker. Invariants of communication channels are used as means of differentiating between the PUE attackers from legitimate PUs</td>
</tr>
<tr>
<td></td>
<td>Liu, Ning, &amp; Dai, 2010</td>
<td>-</td>
<td>Novel physical layer authentication mechanism, which incorporates cryptographic and wireless link signatures</td>
</tr>
<tr>
<td></td>
<td>Dabcevic, Marcenaro &amp; Regazzoni, 2012 (our proposed scheme)</td>
<td>Ability to emulate any of the PU’s transmission characteristics</td>
<td>Location integrity checking as means of deciding on the credibility of a user</td>
</tr>
<tr>
<td>Byzantine – providing wrong data to other nodes in collaborative spectrum sensing</td>
<td>Wang, Li, Sun, &amp; Han, 2009</td>
<td>Two operating modes: causing False Alarm attack, or causing False Alarm &amp; Miss-detection</td>
<td>Each user is attributed a suspicious level, turned into a trust value, but also a consistency value</td>
</tr>
<tr>
<td></td>
<td>Min, Shin, &amp; Hu, 2009</td>
<td>Two types of attacks: false-positive and false-negative. The attackers are assumed to be able to estimate the channel occupancy with 100% precision</td>
<td>Double-defense mechanism: the correlations between the reported RSS values using correlation filters are observed and the suspicious nodes are outlined; usage of the weight-combining data fusion rule</td>
</tr>
<tr>
<td></td>
<td>Noon &amp; Li, 2010</td>
<td>Hit-and-run attacker - able to estimate its current suspicious level and adapt its attacking scheme</td>
<td>Novel reputation algorithm - the user is permanently excommunicated once his reputation value is below a threshold</td>
</tr>
<tr>
<td>SJA – sending spurious RF data, disrupting the normal communication</td>
<td>Dabcevic, Marcenaro &amp; Regazzoni, 2012 (our proposed scheme)</td>
<td>The attacker tries to emulate the “good” radio node</td>
<td>Frequency switching algorithm</td>
</tr>
<tr>
<td></td>
<td>Qinggi, Hongning, &amp; Kefeng, 2011</td>
<td>-</td>
<td>Set of general guidelines, e.g. Multi-Objective Programming module verifies all of the reconfigured parameters in each iteration</td>
</tr>
<tr>
<td>OPA – disrupting CR’s learning mechanism</td>
<td>Hernandez-Serrano, Leon, &amp; Soriano, 2010</td>
<td>-</td>
<td>Set of general guidelines for reducing the efficiency of the attack</td>
</tr>
<tr>
<td>Lion attack – multi-layer attack with the goal of causing DoS at the transport layer</td>
<td>Zhu &amp; Zhou, 2008</td>
<td>two types of attacks: DoS attack in multi-hop networks, and the greedy MAC layer behavior</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Safdar &amp; O’Neill, 2009</td>
<td>-</td>
<td>Authentication of communicating CR nodes as the key security feature</td>
</tr>
<tr>
<td>Spectrum trading security issues</td>
<td>Zhu, Suo, &amp; Gao, 2010</td>
<td>Attacker decreases the QoS while declaring that it remains the same</td>
<td>Once it observes illegal behavior, PU decreases the amount of spectrum shared with SU, thus reducing its overall utility</td>
</tr>
</tbody>
</table>
Identification of the possible attacks: DoS; Replay; Jamming in QPs; PUEA; Threats to WMBs; Attacks on Self-Coexistence mechanism

Security sublayer deals with some of the vulnerabilities, mainly through: Privacy Key Management v2; message authentication codes; Advanced Encryption Standard

| 802.22-specific | Biao & Park, 2008 | Table 1: Summary of the threats to Cognitive Radios and the proposed solutions

Primary User Emulation Attacks

Two types of users can be differentiated in CRNs: Primary Users (PUs) and Secondary Users (SUs). The main premise of the opportunistic spectrum access lies in the SUs’ ability to access the channels normally assigned to PUs when they are free of occupancy. In order to decide whether the channel is momentarily free, or is in use by the PU or the other SU, the cognitive radio needs to perform spectrum sensing (alternatively, two other methods – geolocation/database and beacons are proposed in the literature, and were addressed in the subsection “Alternative spectrum occupancy decision methods and the related security threats”). Several spectrum sensing approaches, such as energy detection, cyclostationary feature detection, second-order statistics detection, filterbank-based detection, etc., have been proposed up to date, each with its advantages and disadvantages in terms of ease of implementation, decoding complexity and sensing accuracy in various channel conditions. In case that the CR decides that the specific channel is momentarily not in use by the PU, it competes with other potentially present SUs in order to acquire the rights to access the channel. Furthermore, once that it has been assigned the rights to use the channel, the CR will still need to periodically perform spectrum sensing and, should it sense the presence of a PU, vacate the channel immediately.

Primary User Emulation Attack (PUEA) is a type of attack where a secondary user falsely advertises itself as a primary user, either to acquire exclusive right to the spectrum occupancy, or to cause Denial of Service (DoS) within the network. Depending on the spectrum sensing technique that the legitimate SUs use, the adversary emulates certain characteristics of a PU – i.e. in CRNs where SUs use energy detectors, the PUE attacker will try to create signals of similar power, whereas in networks with feature-based detectors the attacker will emulate the corresponding feature of the PU. To counter the PUE attacks, the appropriate defense scheme able to distinguish between real and mimicking PUs needs to be implemented within the network.

One of the aggravating factors in devising such a scheme is Federal Communication Commission’s instruction that „no modification to the incumbent signal should be required to accommodate opportunistic use of the spectrum by SUs“. PUEAs have arguably been given the most attention in the literature out of all the threats specific to CRNs. The PUEA-defense contributions can be divided into those where the locations of the PUs are supposed to be known a-priori, such as in cases when PUs are for example TV towers or base stations, and those where the PUs' locations cannot be assumed to be known beforehand.

Authors in (Chen, Park, & Reed, 2008) propose a location-based method, applicable to the network where PUs are TV towers, with high transmission power and high transmission range. The authors model a CR attacker capable of altering its transmit power, modulation mode and frequency. Two types of attacks are possible: in the first one, the attacker alters the RSS
measurements by changing the transmit power, whereas in the second one, the attackers inject false data to the localization system.

To counter such attackers, they propose a scheme that „estimates a location of the signal source and, if it deviates from the known location of the TV towers and the signal characteristics resemble those of primary user signals, then it is likely that the signal source is launching a PUE attack“, assuming that „it would be infeasible for an attacker to mimic both the primary user signal’s transmission location and energy level since the transmission power of the attacker’s CR is several orders of magnitude smaller than that of a typical TV tower“. The scheme consists of three steps: verification of signal characteristics, RSS measurement, and localization of the signal source.

Simulation results show the effectiveness of the scheme, designed for the networks in which PUs have fixed locations and high transmit powers. In cases of mobile PUs with relatively small power (directly leading to higher RSS fluctuations), alternative approaches need to be used.

In (Chen, Cooklev, Chen, & Pomalaza-Raez, 2009), authors propose another location-based method for dealing with advanced PUE attackers. The modeled attacker is capable of applying the estimation techniques to enhance its performance, i.e. it „can employ a maximum likelihood estimator to infer the transmit power of the primary user and a channel parameter, and use the inferred parameters and a mean-field approach to generate primary user emulation“. It is assumed that the attacker has the location information of all the entities in the network. The authors also assume the use of energy detectors as spectrum sensing mechanisms, meaning that the attacker needs to try and transmit signals whose energy will be as similar as possible to the one transmitted by the legitimate PU, from the viewpoint of the targeted SUs. To do this, attacker estimates the PU’s transmit power and the channel parameter, and then, taking into account its distance to the targeted SU and PU’s distance to the SU, launches a PUE attack.

The designed defense mechanism lies on the presumption that the attacker cannot successfully emulate the channel features. Invariants of communication channels are used as means of differentiating between the PUE attackers from legitimate PUs.

The simulation results show that, while such attacker can successfully defeat a „naive” detection method, the proposed mechanism successfully distinguishes between mimicking and real PUs with high accuracy.

Authors in (Liu, Ning, & Dai, 2010) have modeled a non-location-based mechanism, which uses a helper node placed proximate to the PU in order to counter PUEAs. The helper node „serves as a “bridge” to enable a secondary user to verify the cryptographic signature carried by the helper node’s signals, and then obtain the helper node’s authentic link signatures to verify the primary user’s signals“. The authors propose a novel physical layer authentication mechanism, which incorporates cryptographic and wireless link signatures. It is assumed that all SUs have reliable ways to obtain the correct public key of each helper node, and that the helper node cannot be compromised by an attacker.

Proposed scheme and simulator for countering PUEA

We are presenting a naive location-based method for identifying PUE attackers, with the assumption of the a-priori knowledge of the locations of all of the users. The method is based on the credibility calculation for all of the SUs, and the final decision of whether the SU is the
actual PU or the PUE attacker is done by comparing its credibility to the predefined threshold for the given SNR level.

The following assumptions were made:

- Each user has the a-priori information of other users’ locations,
- The attackers are capable of emulating one or more of the PU’s features, including the ability to transmit at the same power as the PU,
- Prior to encountering PUE attacker, the CR is ensured to have established communication with the legitimate PU, in order to derive the appropriate threshold value for user classification for a given channel.

The algorithm decides on the credibility of the user in a following way:

- Based on the coordinates on the playground, the distance between the SU (CR) and the legitimate PU is calculated.
- The RSS values of the legitimate PU transmitting a signal at constant power are calculated for different SNR values. The expected distance between the SU and legitimate PU can be calculated from the RSS value.
- The credibility of each user is calculated as the ratio of the real distance (derived from coordinates) and approximated distance (derived from RSS values). This value is used as a „ground truth“, and the threshold value for future user classification is derived from this credibility.
- The RSS values of subsequent users are calculated depending on their distance and transmit power, and their credibility is derived using the previous method. The credibility is then compared to the threshold, where it is decided whether a user is a legitimate PU or a PUE attacker.

It should be noted that the algorithm performs better as more samples from legitimate PUs can be obtained for calculation of the threshold.

In the simulations, AWGN free-space channel with corresponding path loss values has been used in channel modeling. The transmit powers of the legitimate PU and the emulating SU are equal. For calculating the threshold, we have performed Monte Carlo simulations with 1000 iterations, where position on the playground was randomized in every iteration. The threshold is calculated as:

\[ \gamma = 0.995 \times \text{total\_trust} \]

The credibility of each subsequent user is then compared to the threshold and, if its value is higher than the threshold, the user is regarded as a legitimate PU.

Figure 1 shows the distribution of the average calculated credibility over 1000 iterations, versus SNR, whereas probabilities of the correct detection of the legitimate PU, and the successful detection of the attacker are given in figure 2.
Because of the noise power causing high RSS fluctuations in low-SNR environments, the credibility of legitimate PUs is relatively low in such harsh channel conditions. The algorithm fares substantially better in higher-SNR environments. For SNR=15dB, the algorithm is able to correctly identify legitimate PUs with a 98% accuracy, and malicious users
with 92% accuracy, whereas for SNR=25 dB, legitimate PUs are correctly categorized with a 100%, and malicious users with 98% accuracy.

Different results can be obtained for different threshold constraints.

Alongside the aforementioned poor channel conditions, the main vulnerabilities of the algorithm arise when the attacker is close to the real PU. In those cases, either a more complex RSS-based scheme, such as the one previously mentioned proposed by (Chen, Park, & Reed, 2008), or an alternative, non-RSS-based scheme need to be used for the successful detection of PUEAs.

**Byzantine attacks**

Once the sensing part is finished, the CR needs to decide how to use the acquired data in order to correctly estimate the channel occupancy state. While it is possible for each entity to make this decision solely based on their own spectrum sensing outputs, more precise results can be achieved if the users can exchange the information among themselves. This is the idea behind collaborative spectrum sensing, where SUs either send the results of the spectrum sensing to each other, or to a centralized entity which then decides on the channel occupancy and feeds this decision back to the SUs. This way, the correct detection probability of a channel occupancy, potentially impaired due to the problems such as a „hidden node“, equipment malfunction, or poor channel conditions, can be improved significantly.

However, collaborative spectrum sensing also has its drawbacks – besides the increase of computational complexity (in cases where each node has to make the decision for themself based on the data acquired from multiple users) or the need for use of the additional data fusion entity (in cases of centralized collaborative sensing), certain security issues arise as well.

Byzantine attackers send false spectrum sensing information to the other users or the centralized entity, thus increasing the probability of the wrong decision of the spectrum occupancy. Furthermore, a malfunctioning node may unintentionally also cause faulty reports. In both cases, the ability to correctly estimate the channel availability – arguably the most important feature of CRs – can be degraded severely.

Hence, with regards to the type of the misbehaving CR node, the users can be classified as:

- **Greedy** – with the intention of acquiring exclusive privileges to the free channels by constantly sending the information of a channel being occupied,

- **Malicious** – with the intention of causing harmful interference between the other users, or reducing the spectrum usage efficiency,

- **Temporarily malfunctioning** – who unknowingly send incorrect information regarding the spectrum occupancy.

Coming up with a reliable method for countering the byzantine failures imposes itself as a critical task in order for the collaborative sensing to be able to be safely and successfully implemented.
Various strategies for addressing byzantine issues have been proposed in the literature, different from each other mainly with respect to the data fusion algorithm, reputation algorithm and the attackers' special features considered.

Authors in (Wang, Li, Sun, & Han, 2009) propose a relatively simple defense scheme for singling out the malicious user by computing the suspicious level, trust values and consistency values. The authors consider a single malicious attacker, and show how the algorithm, which eliminates the observations from the node marked as malicious, performs depending on the collaborative sensing scheme used. The attacker can operate in two modes: causing False Alarm attack, where it reports a higher sensed power whenever the power is below its set threshold, or causing False Alarm & Miss-detection, where it reports higher sensed power when it's below the threshold, or lower sensed power when it is above it.

Each user is attributed a suspicious level, which is then turned into a trust value. Since the trust value itself is not reliable in cases when there are either not enough observations, or there is no malicious user present, each user is also assigned a consistency value. By eliminating the reports from the users with consistently low trust values, and then using the OR rule for the remaining nodes, the scheme shows satisfying improvements compared to simpler, more straightforward schemes, for both attacking strategies. The main limitation of the scheme is the fact that only one malicious user is considered at any time.

In (Min, Shin, & Hu, 2009), authors propose a double-defense mechanism for the centralized collaborative sensing, which they refer to as the „Attack-tolerant Distributed Sensing Protocol“ (ADSP). Two types of attacks are taken into account: false-positive, classifying a non-primary user as a primary thus increasing the probability of a misdetection, and false-negative, causing failure to detect a primary signal and increasing the probability of the false alarm. The attackers are assumed to be able to correctly estimate whether the PU is using the channel or not at all times, regardless of the decision the centralized entity makes, therefore being able to switch between their attacking modes.

The proposed defense framework „consists of three building blocks:

- Sensing manager that manages sensor clusters and directs the sensors to report their readings at the end of each scheduled sensing period,
- Attack detector that detects and discards (or penalizes) the abnormal sensing reports based on the pre-established shadowing correlation profile,
- Data-fusion center that determines the presence or absence of a primary signal based on the filtered sensing results“.

The mechanism is implemented in a way that the clustered sensors send their RSS values and location information to the data fusion center, which is being done in two phases. First, the correlations between the reported RSS values using correlation filters are observed, and the nodes whose reports appear inconsistent with the others are deemed suspicious, so their reports are not taken into account for making the decision on the channel occupancy. The other line of defense – implemented because of the inaccuracy of the first one when the attackers produce low-strength attacks – is a weight-combining data fusion rule, where weights to sensors are allocated based on their Conditional Probability Density Function (CPDF). This way, the misbehaving sensors are likely to be given low weight factors, meaning that their reports to the data fusion center will be less likely to affect the final decision.
The simulation results show that the proposed algorithm is able to minimize the probability of a false-alarm by up to 99.2% (for the first type of attack), and to achieve the probability of correct detection of up to 97.4% (for the second type of attack), showing significantly better performances than the other algorithms considered.

In (Noon & Li, 2010), authors present a specific type of an advanced attacking strategy, called Hit-and-run, and the corresponding defense mechanism. The attacking strategy is based on the assumption that the attacker is able to estimate its current suspicious level assigned by the data fusion center, and act appropriately. Namely, when it feels that it's suspicious level is high, and there is a potential for it to be expelled from the network, it stops sending false observations, and starts acting honestly. Once it calculates that it's safe again, it re-starts its malicious behavior, and from there continues to use this Hit-and-run strategy. It is assumed that the attacker is aware of the other nodes' reports to the DFC, and can model its report based on this information.

The conventional reputation-based schemes are unable to deal with this kind of attacker, so the authors have proposed a new point-system. The system permanently bans the user from the network once it has accumulated enough negative reputation points, where each negative point is assigned to the user whenever its suspicion level surpasses a pre-defined threshold. By applying the Wald's equality, the algorithm can approximate the expected time for the attacker to reach the threshold, and also the time for the attacker to decrease its suspicion level. By combining these approximations, the time needed for detecting the attacker can be estimated.

For the set number of 10 secondary users in the network, the authors show how the algorithm fares when faced with up to three attackers. As the number of attackers increases, the algorithm needs more iterations for successful detection, however still successfully manages to excommunicate the malicious users.

**Smart jamming attacks**

RF jamming attacks refer to the illicit transmissions of RF signals with the intention of disrupting the normal communication on the targeted channels. RF jamming is a known problem in modern wireless networks, and not an easy one to counter with the traditional “hardware-based” equipment. Since RF spectrum is an extremely valuable asset, whose lessor in most countries is a state itself, RF jamming is typically seen as a property theft, with fines and repercussions for the identified intentional jammers being substantial.

There are many different types of jammers depending on their allocation, ranging from disrupting the signal receipt at the target receivers, to more sophisticated ones, such as deceiving the targets into accepting false information. Software Defined Radios and Cognitive radios bring the prospect for improving both the jamming capabilities of the malicious user, but also developing advanced protection- and counter-mechanisms.

**Proposed scheme for countering Smart jamming attacks and the simulator**
We define a *smart jammer* as a particular type of an attacker that is able to scan the entire spectrum and selectively jam specific channels, thus causing anomalous spectrum usage and actually interfering with dynamic spectrum access techniques (Morerio, Dabcevic, Marcenaro, & Regazzoni, 2012).

The considered *smart jammer* consists of three major components:

- A spectrum sensor, which senses and locates target’s physical channel,
- A spectrum analyzer, which analyzes the sensed spectrum data and, combining it with the prior knowledge of the target channel, consequently devises an action,
- A radio transmitter, which is dedicated to radiating jamming signals.

In our scenario, we are considering a case with an arbitrary number of legitimate mobile Cognitive Nodes (CNs), and one Malicious Node (MN) equipped with a mobile jamming device – the *smart jammer*. This network is controlled by a centralized Data Fusion Entity (DFE) with a fixed location, which collects the following data from each of the SUs in each timeframe:

- Their position (coordinates $x, y$) on the playground,
- Their Received Signal Strength (RSS) value,
- Their transmit frequency.

The *smart jammer* is designed with the following characteristics and capabilities:

- Ability to jam one frequency at the time, but able to alter the jamming frequency every $n$ timeframes,
- Altering its transmit power – specifically, it refrains from transmitting when it approaches the legitimate node, in order to make the DFE think that it is being jammed by the legitimate node,
- Trying to emulate a legitimate node, sending its true coordinates to the DFE.

The DFE continuously calculates the distance between all pairs of users, as well as their RSS value. Whenever the RSS value for a certain user drops below a pre-defined threshold, it assumes that the user has found himself in the jammer-influenced area, initiates the frequency switching algorithm for the given user, and assigns a negative reputation point to the user suspected of jamming. Upon collecting a certain number of negative reputation points, the user is deemed a jammer, all the legitimate nodes are notified of its presence, and its observations to the DFE are disregarded in the future.

The jammer strategically tries to confuse the DFE into thinking that the other nodes are in fact jammers. By ceasing to transmit whenever it gets close to another node, it causes the decrease in the reputation value for the said legitimate node.

A simulator was realized, where the DFE is implemented as a set of C/C++ interacting modules running on an IGEPv2 - a compact ARM-based industrial processor board. The DFE is able to sense signal strength of detected mobile entities and - by comparing the RSS values - has the
ability to detect jammers within the monitored environment. Implemented prototype is able to deal with fixed and mobile jammers - after a jammer is detected, the cooperative mobile entity automatically modifies its operating frequency, as per DFE’s instructions. It is assumed that the frequency switching initialization protocol between the DFE and the cooperative nodes is being done over a dedicated channel, which cannot be jammed.

The scenario consists of a number of entities (agents) carrying a mobile device which is able to transmit and receive data at 3 different frequencies (namely 800, 900, and 1800 MHz) to a centralized control center. The agents move intelligently (in a sense that they are able to alter their trajectories in order to avoid the obstacles) throughout the jamming-polluted environment. The considered playground is a virtual depiction of a standard urban environment, 40m x 40m large, and the agents are simulated at moving at a constant speed of 5 km/h. The jammers can be either fixed or mobile, and their emitted signal strength follows the Rayleigh distribution with fixed parameters. Fixed jammers’ positions and characteristics are stored in an XML file, which is loaded in the setup stage together with the map of the ground. An example of a scenario with 2 moving agents (Agent1 and Agent2) originally transmitting at the frequency of 1800 MHz, and three fixed jammers (J0 - J3) jamming at 800 MHz, 800 MHz and 1800 MHz respectively, with their respective radii of sensing and influence is depicted in Figure 3.

The agents periodically send a single radio data to the control center, where the running cognitive node receives and processes it.

Radio data sent by an agent contains the following information:
- Position of the agent \((x, y)\) on the mapped ground: this is generated by the trajectories simulator. It simulates a GPS sensor on the mobile device. If video monitoring of the ground area is available, positioning data coming from the tracker can potentially be fused with the GPS data in order to obtain a better position estimation.

- Frequency of the transmission: initial transmission frequency can be chosen at the beginning of the simulation, whereas information of the updated frequencies are sent in every timeframe.

- Power of the transmitted signal: fixed.

- Possibly detected jammers' estimated power: each jammer has a typical radius (coded in the XML configuration file) of influence, inside which the agent can estimate its power (knowing that the signal strength follows the Rayleigh distribution).

- IDs of the possible neighboring agents (within a fixed sensing radius).

We can also look at a slightly different scenario by introducing a moving jammer: now, an additional agent (Agent3), carrying a jamming device, has been added to the scene. Besides disturbing communication at its operating frequency within its jamming radius, it also transmits spurious data to the DFE regarding its position. A scenario with 2 moving agents transmitting at the frequency of 1800 MHz and one Jammer transmitting at the same frequency, with their respective radii of sensing and influence is depicted in Figure 4.

![Scenario with mobile jammer (intruder)](image)

Frequency switching process for one of the agents (Agent1) as a function of time, and depending on the jamming power of the nearby jammers is given in Figure 5.
The same process for both agents (Agent1 and Agent2) for the modified (mobile-jammer) scenario is given in Figure 6. As can be seen, in this case the frequency switching only occurs once for each of the agents: since mobile jammer doesn't have the capability of jamming multiple frequencies, there is no reason for agents 1 and 2 to deviate from their newly-set frequencies once they start transmitting at a frequency not influenced by the malicious agent.

Figure 5: Frequency switching depending on the jammer power (two agents and three fixed jammers)

Figure 6: Frequency switching depending on the jammer power (mobile jammer)
The radio data reception represents, from the node point of view, the "sensing" stage of the cognitive cycle. The agents' mobile terminals are equipped with sensors which monitor the environment, sending a radio survey (radio sensors) and positioning (GPS sensor) information to the cognitive node.

The cognitive node - acting as a data fusion center - then analyzes all the information received from each agent. For each agent, the signal-to-noise and distortion ratio (SINAD) of the received data packet is computed. Also, agents' relative positions are compared, and by the means of the voting algorithm, rankings are assigned to each agent's ID. Then, intruder's position and ID are worked out.

In the decision stage, the SINAD datum is compared to an acceptable (fixed to 10 dB) threshold. If the communication with an agent under the jamming influence proves to be below the acceptable threshold, a suitable strategy is chosen in order to schedule a change in the transmit frequency.

The "action" stage leads to the change in the state of the system. As was previously explained, this module implements the active interaction of the system towards the surrounding environment or towards itself: the action of changing frequency is selected based on the strategy ST chosen during the previous step. Hence, detection of the intruder does not trigger a decision and a subsequent action in the cognitive cycle. Instead, the information relative to the malevolent agent is transmitted to the third party agent, which in real-life application could, for example, display data on the mobile devices, thus leaving the decision step under human control. Alternatively, a learning-based-on-experience strategy could be deployed within the DFE in the future perspective.

**Alternative spectrum occupancy decision methods and the related security threats**

Besides spectrum sensing, two other methods have been proposed by the NPRM - Notice of the Proposed Rule Making - Unlicensed Operation in the TV Broadcast Bands (Check, Scott, Mace, Brenner, & Nicoll, 2004) as alternative ways of acquiring spectrum occupancy information: geolocation/database and beacon signals.

Overcoming some of the drawbacks of the spectrum sensing approaches (which vary depending on the sensing technique used) - such as possibly long sensing periods, unknown/incomplete waveform information, or bad channel conditions - geolocation/database approach has recently sparked interest in the CR research community. This approach requires the SU to have a perfect awareness of its location, and to be able to access the database containing the list of the currently available frequencies at a given location. One particular feature makes usage of the geolocation/database approach especially appealing from the regulatory point of view: the possibility of easier management of the frequencies or frequency bands that the lessor wishes to declare as “available” or “busy” at any given time.

Naturally, this approach brings its own set of security issues and concerns, primarily:

- Continuous database accessibility – ensuring that the database is always „up-and-running“, and updated with the list of (un)available frequencies is a necessity.
• Database management and updating – since databases need to be regularly updated, there is a need for a reliable mechanism for the processes of updating and downloading the updated content to the cognitive device.

• Database tampering – while originally the communication between the database and the SU is intended to be one-way (SU downloading the content from the database), ensuring that malicious content cannot be uploaded by the SU by deploying anti-tampering methods is paramount.

• Database emulation - similarly to PUEA, if the SU retrieves information from a source pretending to be a spectrum lessor in a given geographical area, it can make wrong estimations of the spectrum occupancy of a given frequency band – i.e. it may try accessing a channel currently marked as „busy“ by the spectrum lessor (malicious attack), or may refrain itself from accessing a channel that is in fact marked as „available“ (selfish attack).

• Providing false geolocation information – whereas many CRs are expected to have direct geolocation capabilities due to the embedded navigation systems, such as GPS (Global Positioning System) or GLONASS (Globalnaya Navigatsionnaya Sputnikovaya Sistema), there might be instances where this is not the case, or where the navigation system is malfunctioning. In this case, CRs may have the capability of finding out their coordinates by triangulation with other cooperative or non-cooperative devices, which opens up the possibility of providing false data, thus causing the targeted device to perform the triangulation erroneously.

Beacon signals method refers to the usage of beacons as means of providing the prospective SUs information of the available frequencies in their proximity. SUs tune to a dedicated channel in order to extract the information of the spectrum availability from the beacons, and then decide upon the optimal way to proceed. In the case of the absence of the beacon, the SUs should refrain themselves from using the spectrum opportunistically.

The main issues from a security and privacy standpoint that impose themselves are as follows:

• Beacon emulation – emulation attacks are a common security issue in CRNs, regardless of the approach taken towards realizing the spectrum occupancy. That being said, Beacon signals seem particularly prone to such attacks, since they represent a single point of failure. The attacker may intercept the beacon, alter its parameters and/or predict the behavior of the cognitive users.

• Security of the Common Control Channel – with the assumption that the beacons are being transmitted over a dedicated channel, it is necessary to address the related security problems. CCC-related security issues and the proposed defense mechanisms are discussed in the subsection „Other attacks and threats“.

• Beacon misinterpretation – one of the challenges lies in preventing the beacon to be received outside of the designated geographical area, thus causing the incorrect interpretation of the contained information, e.g. a SU receiving a beacon from the neighbouring cell, and mistakenly concluding that the channel X is free for accessing opportunistically. Furthermore, in case of multiple beacons co-existing in the same
location at the same time, there is a problem of deciding upon which is the one carrying the correct information for a given geographical spot. Whereas beacon designs have been proposed in the literature, such as (Lei & Chin, 2008), architecture dealing with the aforementioned security problems is still an open issue.

**Threats to reputation systems**

In Cognitive Radios, usage of the reputation systems has a particular purposefulness in the networks where some sort of collaboration between the users exists such as in the context of collaborative spectrum sensing. Whereas threats to the reputation systems were somewhat covered in the subsection “Byzantine attacks”, it is useful to provide a more detailed coverage of the potential attacks and issues. Authors in (Sun & Liu, 2012) have given a detailed comparison of the attacks on feedback-based reputation systems, recognizing:

- **Whitewashing and traitor attacks** – whitewashing attacker is able to discard its current ID, and re-enter the system (network) with a new ID. Traitor attacker is able to restore his reputation score by behaving non-maliciously for a certain time period (see “Hit-and-run attacker” under “Byzantine attacks”). The authors propose increasing the cost/complexity for acquiring a new user ID, as well as low initial reputation for new users as a defense strategy against whitewashing. Against traitor attacks, the adaptive forgetting scheme with the fading factor is proposed.

- **Attacking object quality reputation through dishonest feedback** – refers to providing false feedback information in order to lead the reputation system towards the erroneous decision. The authors recognize three different approaches towards tackling dishonest feedback attacks:
  - Increasing the cost of dishonest feedback – users are needed to have certain credentials to be able to provide feedback.
  - Detection of dishonest feedback – deployment of a defense scheme that detects dishonest feedback based on the majority rule, i.e. the feedback that significantly differs from the majority’s opinion is disregarded
  - Mitigating the effects of dishonest feedback – feedback of users with lower feedback reputation will have less impact on the overall score. There are several proposed methods for calculating the feedback reputation of a user, such as computing a weight of a user’s feedback in the feedback aggregation algorithm as the inverse of the variance in all of his or her feedback.

- **Self-promotion attacks** – attackers can provide honest feedback for the objects they are not interested in – for example, in case of collaborative spectrum sensing, for frequency bands that they are not interested in opportunistically accessing. For countering self-promoting attacks, the defense schemes used against whitewashing and traitor attacks can be applied.
Complicated collusion attacks – in order to enhance the efficiency of attacks and reduce the probability of being detected, attackers may collude. The authors differentiate two types of complex collaboration attacks:

- Oscillation attack (Srivatsa, Xiong, & Liu, 2005) – malicious users are divided into different groups, each group performing different role at a given time – i.e. while one group focuses on providing dishonest feedback, the other may focus on improving its reputation by providing honest feedback to the non-targeted objects. The focuses of these groups may switch dynamically.

- RepTrap attack (Yang, Feng, Sun, & Dai, 2008) – malicious users focus on breaking the “majority rule” of an object by making the majority of feedback for the given object dishonest.

For countering the complicated collusion attacks, two different defense schemes were proposed: a scheme using temporal analysis, which explores the information in the time domain (e.g. changing trend of rating values), and a user correlation analysis, which aims at finding the patterns between the malicious users.

Other attacks and threats

Several other attacks that are directly related to the cognitive functionalities of CRs have been devised, and studied in the literature.

Objective Function Attacks (OFA) are aimed at disrupting the most complex of the CR’s functionalities – its learning mechanism. Learning mechanism will typically be on top of triggering the reconfiguration process of most of the reconfigurable radio parameters, such as frequency, modulation type, power and coding rate, in order to improve the overall performance – e.g. increase of the data-rate, decrease of the energy consumption, or enabling or disabling certain security protocols and functions. The malicious users can try and tamper with some of these parameters, in order to prevent the CR from adapting in an optimal way.

To counter OFAs, (Qingqi, Hongning, & Kefeng, 2011) propose a simple method called Multi-Objective Programming module, which verifies all of the reconfigured parameters. The model is based on Particle Swarm Optimization (PSO) – a computational method for solving optimization problems in which software agents move through the problem space, trying to improve the candidate solution. Upon reconfiguration, the algorithm is supposedly able to detect the attackers, and reset the parameters to previous state.

Lion attack is a cross-layer attack characteristic for CRNs, where the malicious node targets the physical layer, in order to cause DoS at the transport layer. The attacker performs either a PUEA, or a jamming attack, thus forcing the SU currently using the channel to perform frequency handoff. Because of the high latencies of data flow within the TCP protocol, the situation where the transport layer is unaware of the temporary disconnection due to the handoff can occur. The transport layer keeps streaming data, which is then not transmitted, but queued at the lower layers, leading to certain TCP segments being delayed, or even permanently lost, and the throughput suffering substantially.
Authors in (Hernandez-Serrano, Leon, & Soriano, 2010) evaluate the impacts of Lion attack on TCP performance, validating its efficiency through simulations. The authors provide general guidelines for reducing the efficiency of Lion attacks, namely freezing the TCP connection parameters during the frequency handoffs, and deploying the CRN-adapted intrusion detection systems.

Common Control Channel (CCC) is expected to be present in most Cognitive Radio Networks, both centralized (enabling communication between base station and SU) and distributed (for the communication between SUs), and as such imposes itself as one of the potential points of attack. The attacker can, for example, forge the MAC frames in multi-hop networks, where there is no mechanism for the MAC frames authentication, thus causing DoS.

In (Zhu & Zhou, 2008), the authors analyze two types of attacks on the CCC: the aforementioned DoS attack in multi-hop networks, and the greedy MAC layer behavior, where a “CR device is being reconfigured to exploit implicit fairness mechanisms in lower-layer wireless network protocols for the advantage of that CR device’s performance”, or where “the greedy nodes refuse to transmit data to legitimate nodes so as to obtain better channel allocation for themselves”.

Authors in (Safdar & O’Neill, 2009) propose a framework for a secure Common Control Channel in multi-hop CRNs, suggesting that “channel announcements, selection and reservation takes place in the common control channel, whereas data exchange in the selected data channel between two cognitive radio nodes occurs in the data channel part of the MAC super frame”, and pointing out to authentication of communicating cognitive radio nodes as the key feature of the framework.

Spectrum trading refers to assigning the RF spectrum through administrative means, allowing a spectrum license holder to directly control the process of spectrum lease or a sell to a non-licensed user. As such, it is one of the most interesting capacities of Cognitive Radios from the license holders’ point of view. Whereas security of spectrum trading by itself has mainly regulatory, as opposed to technical, significance, thus differing from the mechanisms considered throughout the rest of the chapter, it is useful to point out towards such mechanisms as well.

Authors in (Zhu, Suo, & Gao, 2010) have addressed the security aspects of the spectrum trading by using a game-theoretical approach, formulating the process as a reversed Stackelberg game. The authors assume cooperation between a PU and a SU, where:

- The primary base station (BS) communicates with the primary users, and trades unused frequency spectrum with the secondary network. Then, the secondary BS could act as a relay for the primary network, where a contract is required between the primary network and the secondary network to ensure a QoS level in the relay work. The secondary network can gain some utility from the relay work. Moreover, unused frequency spectrum in secondary network could also be leased to secondary users. (Zhu, Suo, & Gao, 2010)

Applying a game theoretical concept to a wanted model and searching for its Nash equilibrium(s) requires defining a finite set of actions that each of the players can take, as well as each player’s utility functions. The authors define five factors that compose PUs’ utility function: satisfaction of its transmission, profit from selling spectrum, gain and payment from the SUs’ relay work, and performance loss due to the shared spectrum with SUs. SUs’ utility is comprised by: gain from its data transmission, profit and cost from acting as relay, and the payment for the purchased spectrum. The observed security issue refers to the scenario where SU tries to cheat.
the primary PU by decreasing the QoS while declaring that the QoS remains the same. The proposed scheme tackles this by continuously supervising SU’s performance parameter and, in case that illegal behavior occurs, the PU punishes the SU by decreasing the shared spectrum with SU, thus reducing its overall utility.

**802.22 standard for CRNs and the related security threats**

The IEEE 802.22 is a cognitive radio standard for Wireless Regional Area Networks, WRANs developed by the IEEE 802 LAN/MAN standards committee, specifying the methods for opportunistic usage of the white spaces in the 54 - 862 MHz TV bands. Following the general paradigms of the Opportunistic Spectrum Access, the 802.22 standard prescribes the set of rules for the OSA, whilst ensuring that the normal operation of the TV services remains undisrupted by the interference. The standard considers two approaches for achieving the knowledge of the spectrum occupancy: spectrum sensing and geolocation/database. Centralized network architecture is defined, where in the case of the spectrum sensing method being used as means for determining the occupancy, secondary base stations are in charge of directly coordinating the cognitive users to achieve spectrum sensing synchronously. The sensing outputs are then forwarded to the centralized entity (data fusion center), which makes a decision on the spectrum occupancy.

Several security threats directly related to 802.22 standard can be identified. Whereas the standard defines the existence of the security sublayer, able to tackle several common security issues, it does not contain any specific technique for protecting spectrum sensing or geolocation information, or the data coming from the database. Examples of potential 802.11-related security threats are (Bian & Park, 2008):

- **Denial of Service (DoS):** attackers create messages for disturbing spectrum sensing and allocation processes. This type of threat is managed by the 802.22 security sublayer through PKMv2 (Privacy Key Management v2) and message authentication codes.
- **Replay Attacks:** the attacker captures and replays the local sensing reports sent by wireless terminals to their base station. This may cause the base station to make incorrect spectrum sensing decision. IEEE 802.22 uses AES (Advanced Encryption Standard) for dealing with this type of attack.
- **Spurious transmissions in QPs:** the attacker transmits spurious data (jamming) in quiet periods (QPs). By transmitting spurious messages in QPs, an adversary can interfere with the various coexistence-related control mechanisms carried out during QPs.
- **Incumbent Signal Emulation:** In PUEAs, a malicious CR transmits signals whose characteristics emulate those of incumbent signals. This type of attack is also known as “incumbent ghosting”.
- **Security Threats against WMBs:** the IEEE 802.11 standard proposes two solutions for detecting the presence of Part 74 devices (i.e., low-power wireless devices, such as wireless microphones, which are licensed to operate in the TV broadcast bands). If Part 74 signals are detected, a wireless terminal sends a wireless microphone beam (WMB) to collocated base stations in its vicinity. The 802.22 standard specifies that each wireless
terminal needs to possess pre-programmed security keys that enable the use of an authentication mechanism to prevent the forgery and modification of WMBs. The security sublayer protects WMBs from replay attacks in the same manner as it protects intra-cell management messages.

• Security vulnerabilities in coexistence mechanism: One of the most significant security oversights in IEEE 802.22 is the lack of protection provided to inter-cell beacons. All inter-cell control messages are vulnerable to unauthorized modification, forgery, or replay.

Being one of the main novelties that the standard defines, the last point warrants somewhat more in-depth explanation. Self-coexistence is a cooperation mechanism performed between the overlapping WRANs with the intention of improving performance and minimalizing interference. In cases where the base station wishes to perform a spectrum handoff to a channel whose Signal-to-Interference Ratio is lower than acceptable, the On-Demand Spectrum Contention (ODSC) protocol is used. The protocol includes transmitting the intercell beacons between base stations with the goal of sharing spectrum occupancy information. However, attackers may disrupt the synchronization and the exclusive spectrum sharing process by sending false, modified or replayed beacons. This is known as the Beacon Falsification (BF) attack.
TOWARDS THE COMPLETE SECURITY FRAMEWORK FOR THE COGNITIVE RADIO NETWORKS

So far, the common threats present in Cognitive Radio Networks, and the suggested countermeasures to them, have been addressed separately. Constructing the complete security framework able to encompass the most suitable security solutions for each of the potential threats is the ultimate task for ensuring the safe and secure operations within the future Cognitive Radio Networks.

nSHIELD (ARTEMIS Joint Undertaking, 2012) is an ongoing European project, whose goal is ensuring the Security, Privacy and Dependability (SPD) in the context of Embedded Systems. The nSHIELD project is, at the same time, a complement and significant technological breakthrough of pSHIELD, a pilot project funded in ARTEMIS Call 2009, as the first investigation towards the realization of the SHIELD Architectural Framework for SPD. The roadmap, already started in the pilot project, will bring to address SPD in the context of Embedded Systems as a “built in” rather than as “add-on” functionalities, proposing and perceiving with this strategy the first step toward SPD certification for future ESs.

One of the main novelties that the nSHIELD structural framework brings is the introduction of a different reference model. In addition to three horizontal layers: node, network and middleware, it will also contain one vertical layer – the so-called “Overlay”. It is exactly overlay that is an enabler for the desired composability of the system, as this is where a set of security agents will be placed, which will then be properly selected depending on the considered scenario. Each security agent is in charge of monitoring the proper selection of the security measurements and parameters on one of the mentioned vertical layer. The measurements observed by each agent are transformed into metadata, and distributed to the other agents. The aggregated metadata allows for the forming the dynamic context, used for deciding which of the actions and algorithms need to be performed and activated at one of the three vertical layers, in order to achieve the desired SPD level.

One of the key features of the concerned radio-based Embedded Systems is the introduction of the so-called “Smart Transmission Layer”, able to receive and transmit a variety of different radio waveforms based on the software used. This sublayer – implemented within the network layer of the system – is to rely on the Software Defined Radio platform which – once equipped with the possibilities of maintaining scenario awareness, detecting possible threats and adapting to the new situations by itself – will evolve towards the Cognitive Radio. Hence, one of the central points of interest of the project is developing the aforementioned complete, secure framework for CRs and CRNs.

Even though the development is still in its early phase, the general ideas have been established. Namely, through a feasible set of hardware-based and software-based security measures, the following is to be achieved within the framework:

- Secure authentication mechanisms,
- Confidentiality,
- Data integrity,
- Accessibility,
Security in Cognitive Radio Networks

- Multimodal strategies for the isolation of adversary nodes,
- Ability to differentiate between adversaries and unintentionally misbehaving SUs.

The security mechanisms deployed in the current wireless networks are usually constructed as a two-fold line of defense, the first one being proactive mechanisms, and the second reactive ones. The proactive mechanisms common to such wireless networks can serve as the foundation for the considered security framework for CRNs. Namely, these include the sets of cryptographic primitives such as Public Key Cryptography and Hash functions for ensuring the confidentiality and authentication within the network.

The more challenging task is finding a way for combining the proposed reactive mechanisms. Advanced Intrusion Detection Systems (IDSs) impose themselves as a means for resolving this task. IDSs have the task of recognizing the unauthorized access or attack attempts, and triggering the appropriate security mechanism.

Furthermore, it is necessary to ensure that the proposed architecture can accommodate embedded systems with different capabilities. The future intrusion detection system shall, once the security risk or malfunction has been detected, evaluate the ES’s capabilities, as well as the required SPD level imposed by the Overlay, and deploy the appropriate security mechanism. Several state-of-the-art security mechanisms for each of the security threats shall be available for the system at all times, with the possibility of the Internet-based scheme updating. A simplified model is presented in the following figure:

![Figure 7: Basic scheme of the Security-aware framework](image)

For example, in cases where the observed ES has only basic SDR capabilities, one of the software tampering protection mechanisms implemented within the Framework should be deployed, depending on the currently demanded SPD level. The SPD level can continuously change during the scenario, depending on the internal states of the system (e.g. battery level),
and the external parameters from the environment (e.g. harsh channel conditions, or approaching an area where certain problematic behaviors have been experienced in the past, such as presence of a jammer). Alternatively, in case that the observed ES is the state-of-the-art CR device, security mechanisms for each of the identified threats at a given time need to be triggered, also depending on the required SPD level.

The current activities regarding the development of the Security-aware framework are focused on devising the algorithms for successfully countering different Smart Jamming strategies. The future work will focus on developing the appropriate algorithms for other SDR-related and CR-related threats studied throughout this chapter, and integrating them within the described constructed framework, ultimately leading to the complete, adaptable security system for the embedded SDR and CR devices.
CONCLUSION

Cognitive Radio, and the most important features associated with it – Opportunistic Spectrum Access and Dynamic Spectrum Access – undoubtedly make for exciting, innovative and above all beneficial research topics. However, the advanced features linked with CRs bring new sets of security breaches and issues, addressing which is paramount in constructing efficient Cognitive Radio Networks.

This chapter has given a breakdown of the main standards, security problems, and corresponding solutions for “traditional” wireless networks, Software Defined Radio networks, and Cognitive Radio Networks, respectively (where each subsequent network inherits the issues found in the previous ones).

Most of the considered security issues stem out from the deployment of one of the spectrum occupancy decision methods, usually one of the methods of spectrum sensing, and the self-reconfigurability of the radios. As such, the main threats to such mechanisms are identified as Primary User Emulation Attacks, Byzantine Attacks and Smart Jamming Attacks. Depending on type of the learning mechanism deployed, a great security hazard is present in the form of the Objective Function Attack, targeting CR’s learning mechanism, which is still a somewhat understudied topic in the community.

Although there is a number of works in the research community where these security issues have been studied separately, there is only a limited number of works that propose schemes for unification and integration of the security mechanisms into a security framework. Building such a framework is one of the tasks of the ongoing nSHIELD project, the basic foundations for constructing which were presented in the chapter.

As the device capabilities and the prospective ideas behind the Cognitive Radio technology continue to evolve, so do the existing threats and attacks, with some new ones arising on-the-go. Because of the numerous possibilities of variations, keeping up with them from a security perspective is often not an easy task, with challenges on multiple fields still unresolved.
REFERENCES


Security in Cognitive Radio Networks


KEY TERMS & DEFINITIONS

Primary User Emulation Attack: Cognitive Radio-specific attack where attacker emulates some characteristics of Primary Users.

Byzantine Attack: Cognitive Radio-specific attack unique to collaborative spectrum sensing, where attacker provides false spectrum sensing information to the collaborating nodes.

Jamming Attack: attack common to all wireless networks, where attacker intentionally sends spurious data on one or more channels in order to disrupt services of legitimate nodes.

Software Communications Architecture (SCA): An open software architecture for SDR systems, also used by the current state-of-the SDR system – Joint Tactical Radio System (JTRS).