Document No.	Security Classification	Date
/pSHIELD/D4.1	Restricted	18.06.2011

Project no: 100204

pSHIELD

pilot embedded **S**ystems arc**HI**tectur**E** for multi-**L**ayer **D**ependable solutions

Instrument type: Capability Project

Priority name: Embedded Systems / Smart Transmission

SPD Network Technologies Prototype

For the pSHIELD-project

Deliverable D4.1

Partners contributed to the work:

THYIA, Slovenia
SELEX Elsag, Italy,
UNIGE, Italy

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2012)		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	X
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Authors and Approvals			
Authors		**Date**	**Signature**
Name	**Company**		
Marco Cesena	SELEX Elsag		
Elisabetta Campaiola	SELEX Elsag		
Ljiljana Mijić	THYIA		
Spase Drakul	THYIA		
Nastja Kuzmin	THYIA		
Carlo Regazzoni	UNIGE		
Lucio Marcenaro	UNIGE		
Shariful Alam	UNIGE		
Luca Bixio	UNIGE		
Lorenzo Ciardelli	UNIGE		
Mirco Raffetto	UNIGE		
Reviewed by			
Name	**Company**		
Approved by			
Name	**Company**		

Modification History		
Issue	**Date**	**Description**
Draft A	14.10.2010	First issue for comments
Issue 1	03.11.2010	Incorporates comments from Draft A review
Issue 2	05.03.2011	Draft
Issue 3	09.03.2011	Draft
Issue 4	21.03.2011	Draft
Issue 5	18.06.2011	Final

Contents

Figures

Glossary

A/D	Analog/Digital
ASIC	Application Specific Integrated Circuit
BCI	Bit Count Integrity
BER	Bit Error Rate
CR	Cognitive Radio
CW	Copper Wire
D/A	Digital/Analog
DSP	Digital Signal Processor
DSSS	Direct-Sequence Spread Spectrum
EHF	Extremely High Frequency
EM	ElectroMagnetic
ES	Embedded System
ESs	Embedded Systems
EW	Electronic Warfare
FEC	Forward Error Correction
FH	Frequency Hopping
GPS	Global Positioning System
HF	High Frequency
IP V4	Internet Protocol V4
LCD	Liquid Crystal Display
LOS	Line Of Sight
LPI	Low Probability of Intercept
MAC	Media Access Control
MESH	Grid Network
MMI	Man Machine Interface
QoS	Quality of Service
Q-PSK	Quadrature Phase-Shift Keying
RF	Radio Frequency
R&D	Research and Development
SCA	Software Communication Architecture
SDR	Software Defined Radio
SPD	Security Privacy Dependability
SS	Spread Spectrum
SW	SoftWare
S/N	Signal/Noise
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
UHF	Ultra High Frequency
USB	Universal Serial Bus
VHF	Very High Frequency
VLAN	Virtual Local Area Network
WCP	Working Cost of Production

This Page is intentionally left blank

1 Introduction

The main goal of pSHIELD is to ensure Security, Privacy and Dependability (SPD) in the context of integrated and interoperating heterogeneous services, applications, systems and devices.

Systems and services must be robust in the sense that an acceptable level of services remains available despite the occurrence of transient or permanent perturbations such as: hardware faults, accidental operational faults, and intentional threats.

The pSHIELD architecture composability relies on the SPD modules. Indeed the pSHIELD architecture is composed by a mosaic of innovative SPD functionalities, each one of the considered layers.

The pSHIELD architecture is able to derive application instantiations of the general framework, selecting statically (at design time) and dynamically (at runtime) the best SPD functionalities for achieving the required SPD levels. In particular, referring to the abovementioned layers, the SPD modules will implement the following functionalities:

- At node layer, intelligent hardware and firmware SPD
- At network layer, secure, trusted, dependable and efficient data transfer based on self-configuration, self-management, self-supervision and self-recovery
- At middleware layer, secure and efficient resource management, inter-operation among heterogeneous networks
- At overlay layer, composability

R&D for embedded security, intended as a system issue that must be solved at all abstraction levels (protocols, algorithms, architecture), will lead, in the framework of this task, to a coherent, composable and modular architecture for a flexible distribution of SPD information and functionalities between different ESs while supporting security and dependability characteristics.

The D2.3.1 describes and classifies the interdependencies between applications and architectures, respect to SPD.

2 Innovative approaches for SPD driven transmission and Trusted and dependable connectivity

In the past few years, the impact of mobile devices in everyday life is continuously increasing as well as the development of advanced and accessible wireless communication services supporting users in their common activities (e.g., voice call, video streaming, web browsing) [1].

Together with new wireless communication technologies and standards, designed to meet the users' demand of high data rate services, new mobile and smart devices have been proposed exploiting the advances in signal processing techniques, hardware platforms and Embedded Systems (ESs) [2].

Historically, radio terminals were designed to perform a single, given task. On the contrary, nowadays, it is required that many wireless services (e.g., Wi-Fi connectivity, global positioning system) can be accomplished on a single radio terminal, reducing life cycle costs.

To this end, software was added to the system designs to increase capability and flexibility, as shown in Figure 3.1 – [3]. This innovative ES, derived by the introduction of software programmable components, are usually known as Software Defined Radio (SDR). Therefore, as an example, it allows to accommodate new standards and new services as they emerge upgrading the terminal software without requiring to develop a new Embedded System (ES) [4].

Recently, the research activities are focusing on the development of intelligent, cognitive radio systems capable to understand and to be aware of the surrounding environment allowing to exploit all the available wireless services by using a single device.

3 Generality of the project

3.1 Scope

The main objective is the implementation of a radio system capable to maintain awareness of the operating scenario, to detect possible threats and to counteract in such a way to assure communications integrity to the maximum possible extent by reconfiguring the single nodes and/or the system itself.

The set composed by awareness, threat detection, re-configurability, and reaction strategies forms what is named a cognitive radio.

3.1.1 Conceptual Approach

The radio system is a collections of nodes connected together through one or more radio channels.

The use of dedicated point-to-point channels makes the radio terminals simpler, but makes the network rigid.

The use of a single, shared channel provides high flexibility of network topology at the expense of higher complexity of the radio terminals.

Ideally a radio system suitable for our purposes should be an infrastructure-less, self-organizing network, where each node is capable to coordinate with the others in order to obtain a “fair” allocation of resources: in other words it is a so called MESH Network.

Our experience shows that the payback of a MESH Network is much higher than the added complexity, particularly where high grade of system survivability and availability are paramount.
For such reasons, for the scope of this work, a MESH network will be assumed.

3.1.2 Smart SPD Driven Transmission: Conceptual Approach

Accordingly with D2.3.1 chapter 3.3.2, Smart SPD information transmission is a feature of pSHIELD system, based on a Network Layer Service, usually called Software Defined Radio (SDR).

An SDR platform will be used to provide smart transmission. It concerns a radio communication software system, implemented on embedded devices. It can receive and transmit a variety of different radio waveforms, based on the software used. It can, also, be integrated easily with hardware security modules.

It allows to accommodate new standards and new Network Layer services as they emerge upgrading the terminal software without requiring to develop a new dedicated Embedded System Device.

The research activities on Network Layer functionalities of Embedded System Devices are focusing on the development of intelligent Cognitive Radio systems capable to understand and to be aware of the

surrounding environment, allowing the exploitation of all the available wireless network services by using a single Embedded System Device.

As an example, a Cognitive Radio (CR) could learn services available in locally accessible wireless computer networks, and could interact with those networks by using its preferred protocols, so the users would not have confusion in finding the most suitable connection for, as an example, a video download or a printout.

Additionally, a Cognitive Radio could select the carrier frequency and choose the transmitted waveforms according to the perceived environment and to reach a given goal, e.g. to avoid interference with existing wireless networks or to maximize the throughput while guaranteeing an acceptable Quality of Service (QoS).

The following picture shows the evolution of the radio network technologies for Embedded System Devices from traditional systems to Cognitive Radios.

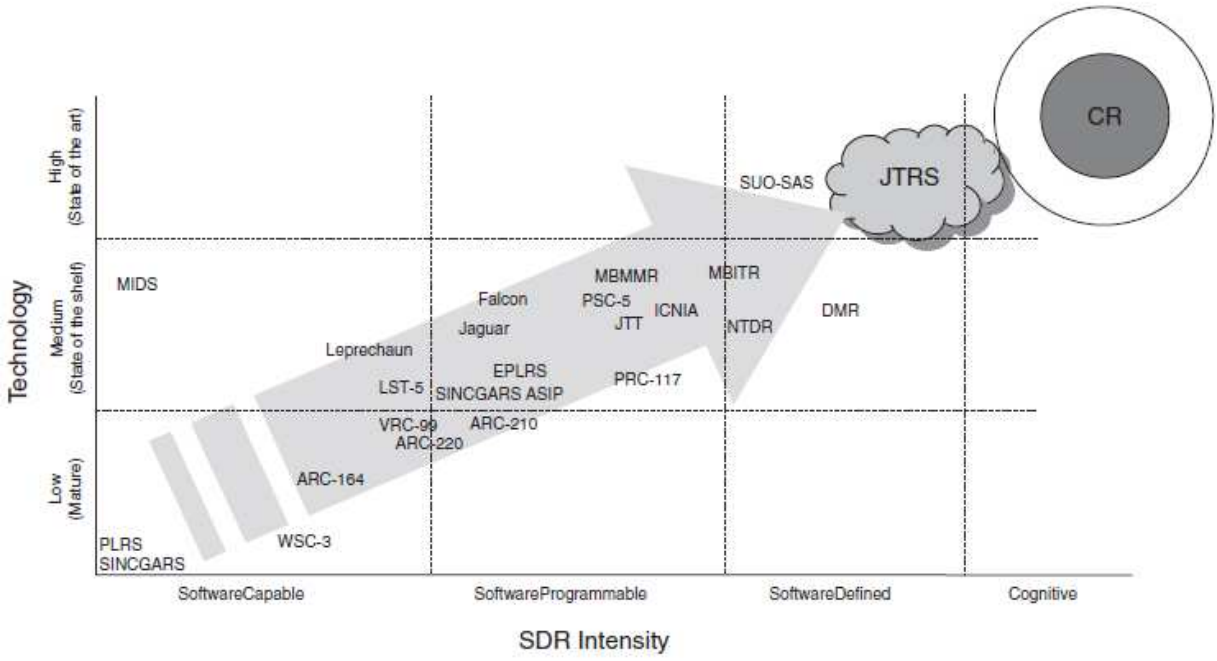


Figure 3.1 – SDR Evolution

3.1.3 Trusted and Dependable Connectivity

Cognitive Radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world) and uses the methodology of understanding-by-building to learn from the environment and to adapt its internal states to statistical variations in the incoming Radio-Frequency (RF) stimuli.

This is obtained by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind: (i) highly Reliable and Dependable communications whenever and wherever needed and (ii) efficient utilization of the radio spectrum.

As it is clear from this definition, the common keywords for an efficient Cognitive Radio are Awareness and Reconfigurability.

In a radio environment, Awareness means the capability of the Cognitive Radio to understand, learn, and predict what is happening in the radio spectrum, e.g., to identify the transmitted waveform, to localize the radio sources, etc.

Reconfigurability is necessary to provide self-configuration of some internal parameters according to the observed radio spectrum.

It is enormously important for both civilian and military applications especially when unforeseen situations happen and some Network Layers services are not available, guaranteeing trusted connectivity.

It is now abundantly clear that the cognitive radios and their capabilities of dynamically maintaining a reliable and efficient communication can be significantly relevant in Security, Privacy and Dependability (SPD) driven applications where it is necessary to dynamically guarantee a high level of trustworthiness.

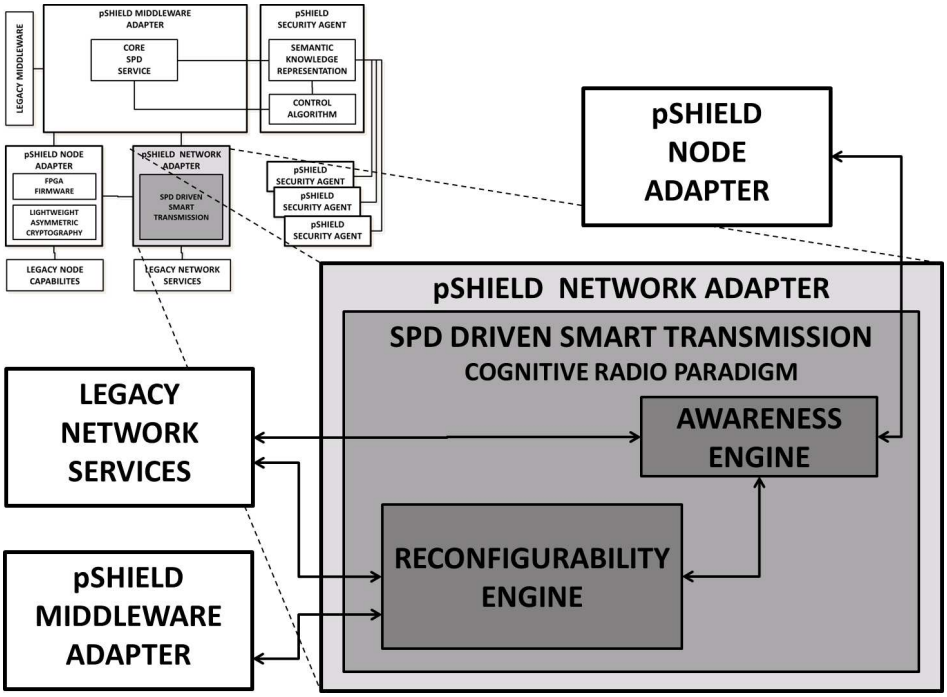


Figure 3.2 – pSHIELD NETWORK ADAPTER conceptual model

As depicted in the above figure and according to the pSHIELD functional component architecture, the Smart SPD driven transmission is obtained applying a Cognitive Radio paradigm based on two main functional components: the Awareness Engine and the Reconfigurability Engine.

Awareness engine consists of spectrum sensing and learning technique. Sensing is done for searching the opportunity of the resources which can be utilized in the absence of legacy users whereas Learning is defined as the process of accumulating knowledge based on the observed impact of the applied action.

Learning can improve reasoning and awareness as well by enriching the knowledge or experience used in reasoning process. Powerful reasoning can improve the efficiency of learning by providing good examples for learning in return. In other words, reasoning and learning in a CR interact and influence each other.

In particular, some Node Layer capabilities (e.g., antennas, cameras) and Network Layer services (e.g. available network resources, radio spectrum, number of active users, transmission protocols and standards, localization, etc.) can be used by the Awareness Engine to acquire a context awareness of the current radio environment.

The reconfigurability engine is responsible of finding an appropriate configuration of the system in response to guarantee the needed SPD transmission (e.g., maximum operating lifetime, maximum robustness, and lowest cost communications) based on the user application quality-of-service (QoS) requirement (e.g., latency and bit error rate) and willingness to share resources and collaborate with other devices in the network.

It is important to note that the Cognitive Radio capabilities are enormously attractive in a wide set of applications for both civilian (e.g., reliable communications, increased data-rate) and military (e.g., detect and decode enemy transmissions) scenarios. Although some encouraging preliminary results have been obtained in some practical environments, some open issues still remain and to obtain a general and multi-purposes cognitive radio is an open research problem. In general the main research challenges in this domain can be reduced to the following:

- Obtain a precise and concise representation of the radio environment (e.g., available radio resources, number of active users in the scene, transmission standard used, source localization) by using some Node Layer and Network Layer information;

- Define the optimal configuration of the Network Layer according to a given goal (e.g., SPD metrics) and the perceived radio environment;

- Develop algorithms and techniques for providing the capability of learning from the experience in order to face unforeseen and unexpected situations (e.g., a malicious user), that means the Embedded System Device's Network Layer is equipped with cognitive capabilities.

3.1.4 Network Model

We will assume that the MESH will be made up by an arbitrary number of terminals.

All the terminals will be the same, i.e. there will not be the need of base stations, repeaters, anchor nodes or other specialized devices; in other words the MESH will be a peer-to peer type.

The MESH will provide support for terminal mobility, both in urban and rural scenarios.

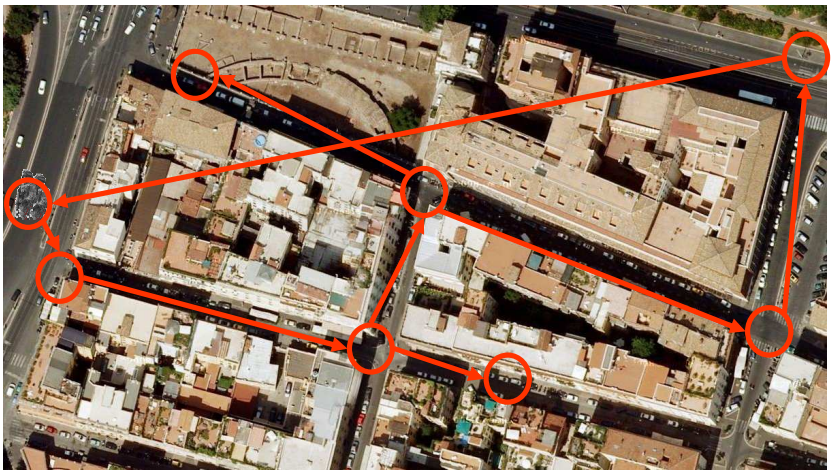


Figure 3.3 – Urban pSHIELD Network

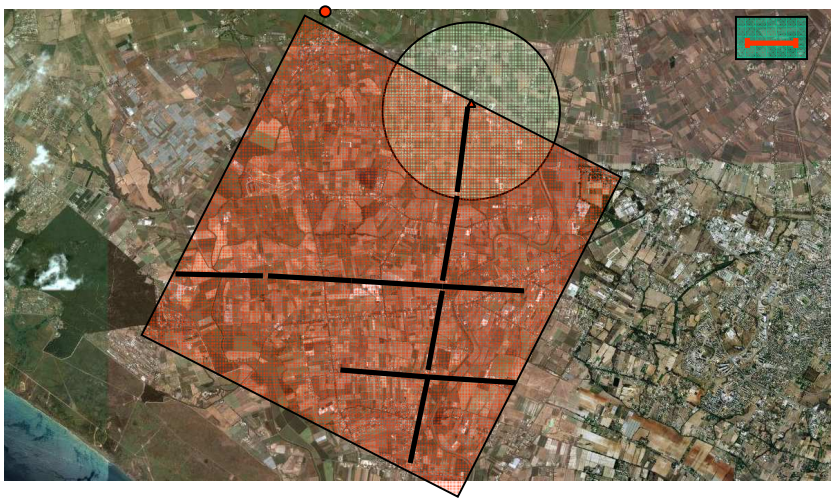


Figure 3.4 – Rural pSHIELD Network

The terminals will share a common radio channel.

We will assume that the radio channel will be sufficiently wide to provide a reasonable throughput and that there will be a large spectrum available for the allocation of the radio channel.

We will assume that the MESH will be capable to accept the entry of a new terminal without affecting overall operation. This is equally true for a terminal leaving the network

We will assume that a terminal can forward the traffic addressed to one node if it is not in the direct range of the source, acting as a repeater. In this way, the terminals have to support data for a single hop or multi hop service.

It will possible to split the MESH in independent sub-networks in case the connectivity is broken at some point. Alternatively, if the number of nodes is increased in a scenario which introduce the computational burden for the network, then deploying the network splitting would be a good solution.

In contrast, it will be possible to merge two MESH groups using the same radio channel if they come close to each other or if the number of nodes decreased significantly for the sub-networks, then the sub-networks may form a new network sharing the same channel.

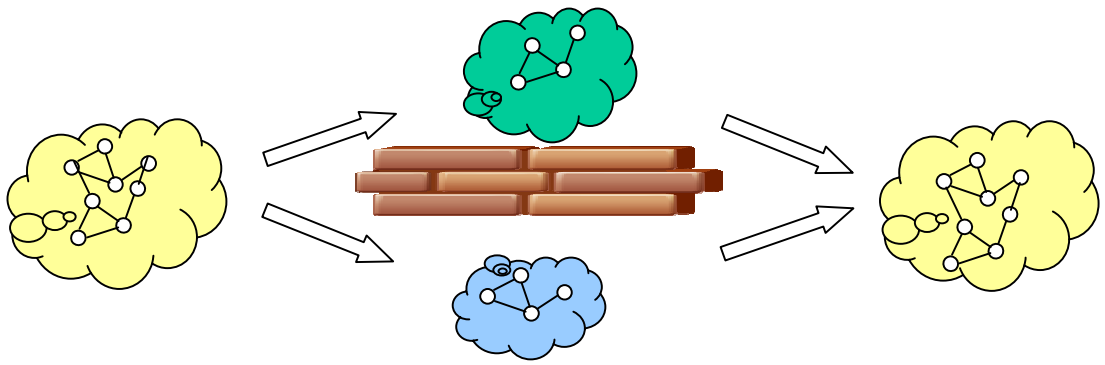


Figure 3.5 – MESH groups using the same radio channel

It will be possible to create independent subgroups that will not interfere to other subgroup.

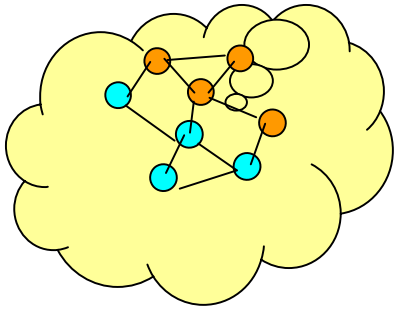


Figure 3.6 – Independent subgroups

We will assume that the MESH will be able to change its topology according to propagation conditions in order to try to keep the connectivity with every terminal.

Finally we will assume that the terminals will be able to modify their transmission parameters in accordance with propagation conditions, traffic requirements, and network topology.

3.1.5 Terminal Model

The “ideal” terminal is a Software Defined Radio (SDR).
This well known kind of radio is a programmable processing platform with a wideband RF front-end, capable to implement a large number of waveforms by loading and executing proper algorithms.

Waveform may be changed at run time.

The platform will provide all the physical and logical resources necessary for the waveform to operate: user interfaces, configurable logic, DSP, A/D and D/A conversion, RF, power supply, MMI, etc.

The waveform itself will provide the physical and upper layers of the communication protocol, including MAC, routing, security.

MAC will discipline the access to the radio channel, while routing will provide forwarding of user data from the source to the other nodes, keeping trace of the evolution of network topology.

The terminal will be able to implement all the functionalities described in previous paragraph.

In addition the terminal will provide sensor and actuators needed for gaining awareness of the operating scenario, for data protection, for the evaluation of possible threats and to put in place proper countermeasures.

3.2 System Integrity

Translating the generic statements of previous paragraphs, let's see how the system will provide:

- situation awareness
- threat recognition
- countermeasures

or, in other words, system integrity. Within the system integrity, it can take decision while observing the scene also can tackle the challenges commencing in the scene. The sections of the building blocks is described in the following sections.

3.3 Situation Awareness

Situation awareness is the collection and correlation of several data that is employed at the node and the network information about current versus expected performance. The cognitive node should be updated through the radio parameters i.e., signal quality, connectivity and EM scenario, etc. The cognitive node provide the instructions to the agents inside the system as per situation awareness messages.

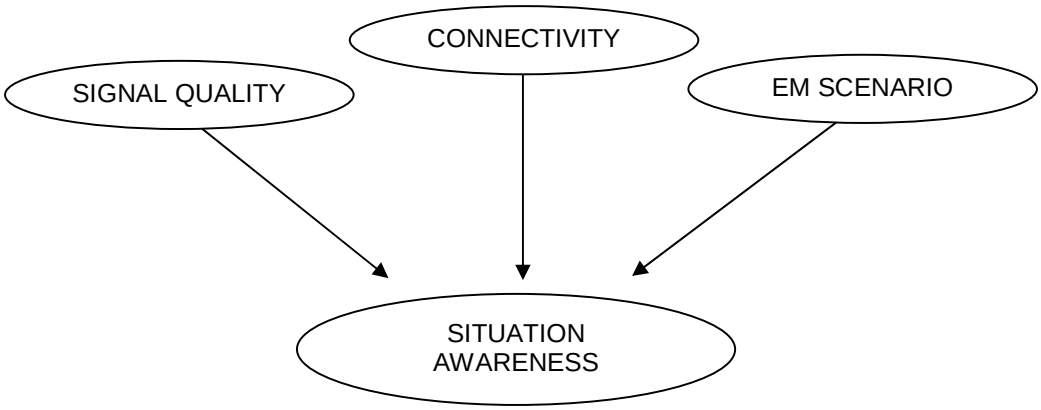


Figure 3.7 – Situation Awareness

3.3.1 Signal Quality

Signal quality may be evaluated in real-time by taking measurements of relevant parameters of received signal:

- Signal to Noise Ratio, SNR
- Bit-Error Rate,BER
- Received Power

Those parameters are made available by the physical layer of the terminal.

3.3.2 Connectivity

Connectivity is provided by a routing table containing continuously updated information about which terminals are visible, directly or through repeaters; this gives the logical topology of the network. The routing table is updated periodically according to the situation awareness messages received by the cognitive terminals.

Routing table is part of the network layer of the waveform.

Such information may be correlated to geo-reference data provided by e.g. a GPS receiver co-located with the terminal.

Associating those data with a geographical information program it is possible to obtain actual deployment of the terminals on the terrain

3.3.3 .EM Scenario

Evaluation of EM scenario encompasses different techniques.

First of all the connectivity and geo-reference data could be forwarded to an EM calculator (like Radio Mobile or similar) in order to evaluate expected signal levels for each link.

Further information may be collected by spectral analysis.

Spectral analysis may be performed by means of a sideway wideband receiver that provides information about other signals existing in the band of interest.

Sideway receiver may be an actual device or the terminal itself may be used.

For instance the waveform might provide “observation windows” in which all the terminals could scan the spectrum searching for possible interferer.

Alternately the terminal could be deliberately sent in scanning mode under network management control.

Again, if the terminal features a wideband Rx front-end, it could take “snapshots” of the received spectrum and provide raw data for off-line processing.

The pilot demonstrator of pSHIELD uses the Sun SPOT sensor platform as micro node. Sun SPOT is a useful platform for developing and prototyping application for sensor network and embedded system. Sun SPOT is suitable for application areas such as robotics, surveillance and tracking.

3.4 Threat Recognition

Threat recognition is the process of evaluating current level of performance to decide, based on the instantaneous measurements themselves or with the aid of additional information and/or processing, if the terminal/network is subject to unintended interference or to an hostile action.

Threat recognition is generally a complex matter: a receiver can provide a limited set of information about the received signal; a clever understanding of propagation effects, together with thorough knowledge of the behaviour of the receiver and the ability to correlate data coming from other sources are needed.

It is impossible here to give a complete description of any possible threat as there are lot of possibilities likely to occur for the radio signals, but just some simple examples may provide insight of the problem.

Assuming that the received signal withstands sudden increase while signal quality drops, returning to normal level after a while one may infer that a pulse jammer is attacking the receiver.
Otherwise, sometimes it happens if the node experiences a signal strength hole (SS hole).

If signal quality and signal level drop, it may be assumed that the signal is fading away, so no countermeasure should be activated.

If signal level remains constant while signal quality drops, one could infer that a CW, noise, or modulated interferer reached a level sufficient to affect signal quality; the matter is to understand if the interferer is unintentional or hostile.

Some interferer have a clear signature, other are more elusive.
In any case a large effort should be devoted in building a threat knowledge base.

The knowledge base is fundamental for a cognitive system: associating historic, geographical and electromagnetic data, the system will build an incremental database of known threats and subsequent actions that can be used when similar conditions are experienced, making decision process faster.

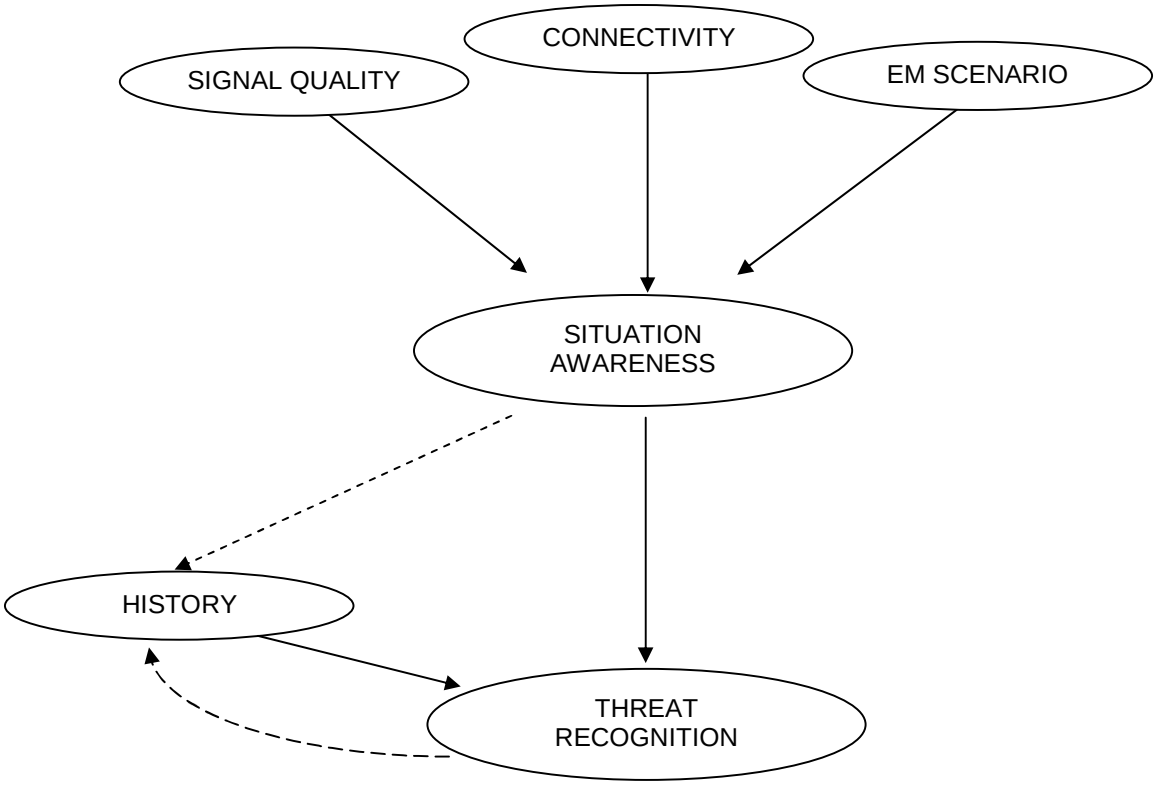


Figure 3.8 – Threat Recognition

3.5 Countermeasures

The system will provide countermeasures to cope with possible threats.

Some countermeasures are of preventive type or as a precautionary measure, i.e. they are always deployed even in the absence of a threat.

Other measures are activated as a reaction to an attack/threat. If a cognitive terminal experiences the presence of a jammer in the considered scene, so the cognitive terminal can reconfigure its radio parameters to avoid the hazards introduced by the jammer.

In order to better recognize the level of threat, the cognitive terminal can analyze data from its history.

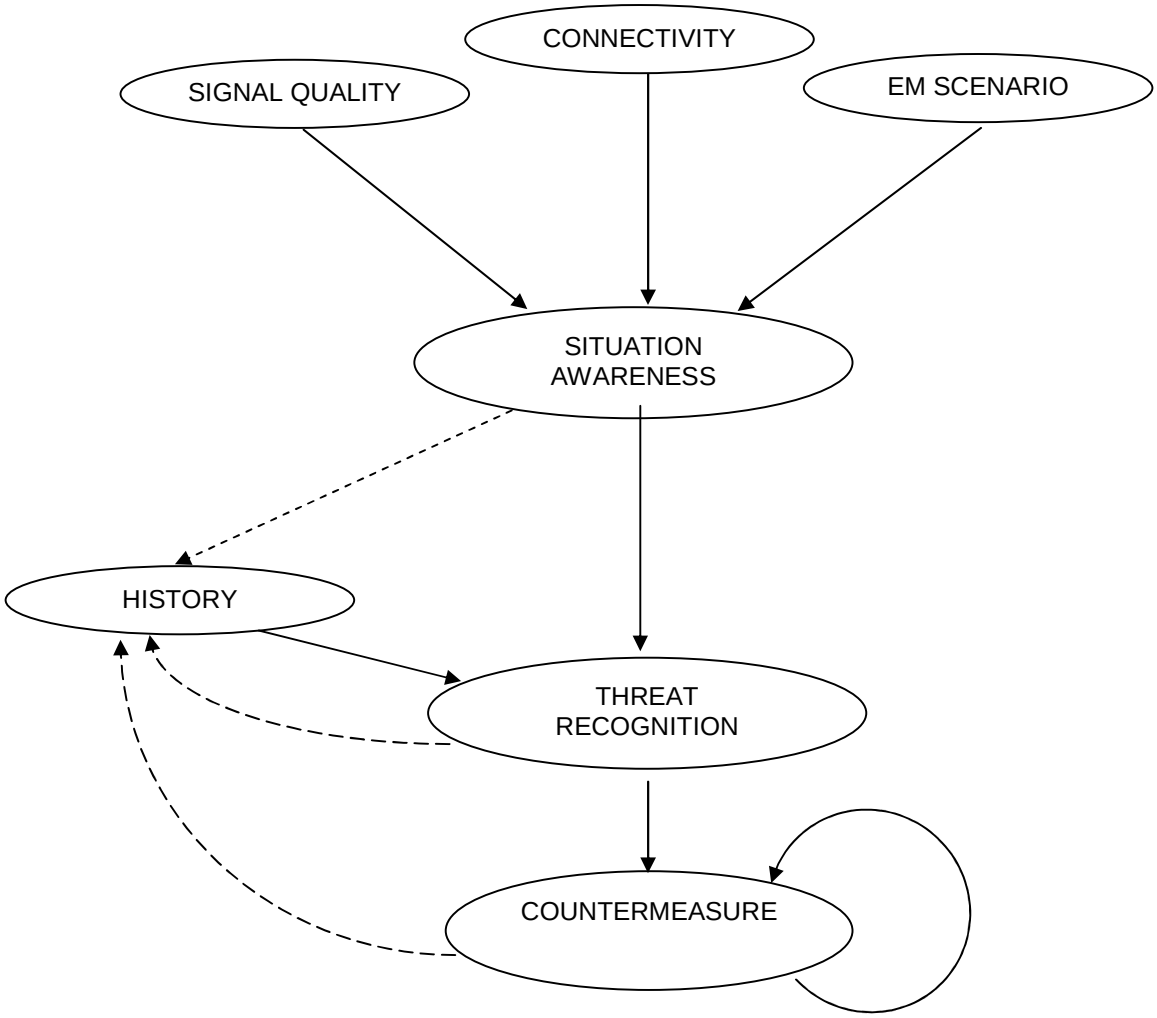


Figure 3.9 – Countermeasure

Let us consider 2 jammers present in a scenario of different frequencies. If an Agent experiences a jammer inside the scene, the cognitive terminal give feedback to the agent to shift a suitable frequency and proceed to communicate.

3.5.1 Preventive Measures

Password protection will take care of unauthorized user trying to operate a terminal.
Unsuccessful login attempts may be logged and transmitted to the network.

Authentication service will prevent the connection of an unauthorized terminal to the network.

Deceitful network entry may be logged and forwarded to the network.

Proprietary waveform formats will make interception and demodulation of the signal difficult.
Payload encryption will be adopted in order to protect user data against unwanted reception.

Anti-tamper measures will be implemented to avoid exploitation of a lost/stolen terminal.
Anti-tamper may erase crypto keys and other sensitive information.

3.5.2 Reactive Countermeasures

The field of countermeasures is wide and is an Electronic Warfare matter.

The fundamental steps in EW are:

- don't be detected
- resist
- escape
- give up....

Several countermeasures are embedded in the terminal, i.e. they are exercised autonomously by the device; some others may need to be coordinated by network management.

Every countermeasure adds a certain degree of complexity to the radio terminal and/or to the network.

3.5.2.1 Don't be detected

A set of techniques, falling under the name LPI (Low Probability of Intercept) are normally adopted.

The simplest one consists in regulating transmitted power to the minimum level compatible with a predefined signal quality.
If signal quality drops, the remote transmitter(s) is asked to increase its output to restore signal quality.

If signal quality increases, the transmitter is asked to lower its output to keep emission to a minimum.

This technique works pretty well in p-t-p links, in fixed p-m-p systems, and in cellular systems while is rather difficult to adopt in infrastructure-less mobile networks, particularly in urban environment.

Adoption of spread spectrum (SS) techniques makes detection or tracking harder.

A DSSS (Direct Sequence Spread Spectrum) transmission is harder to detect than a CW transmission.

A FH (Frequency Hopping) is not hard to detect but is hard to track.

3.5.2.2 Resist

Several receiver hardening measures may be adopted to increase resistance to interferer.

Narrowband channel filtering, high linearity front-end, FEC are helpful in increasing receiver resilience.

Additional countermeasure is constituted by spatial filtering, i.e. adoption of directive antennas or even better, null-steering antennas.

Null-steering antennas are phased array in which the directivity diagram can be actively modified in order to place nulls in the direction from which the interferer comes.

On the other hand null- steering antennas are complex and expensive and do not fit well in mobile and/or handheld radios.

A technique that demonstrated effective against pulse jammers is Bit Count Integrity hardening.
This technique cannot avoid the loss of data during the attack, but makes recovery faster and minimizes loss of synchronization issues, keeping received clock stable for relatively long periods in the absence of received signal, in order to delay as much as possible the eventual bit-slip in the downstream.

Other possibility is to change waveform parameters, switching to a more robust modulation format, or lowering transmission rate to reduce bandwidth; in such way the sensitivity to jammer is somewhat reduced.

3.5.2.3 Escape

Sooner or later a hostile interferer will succeed in overwhelming wanted signal.

In this case the best countermeasure is escape.

A simple frequency evasion scheme may be adopted in order to counteract “dumb” jammers.

SS techniques, like FH, provide additional protection making difficult to track the signal.

SS techniques provide an additional amount of protection thanks to the process gain resulting from the enlargement of the transmission channel.

Nevertheless SS techniques add complexity to the synchronization circuits.

3.5.2.4 Give up

Provided that there is not a countermeasure that can cope with every threat, the last resource is to stop transmission and try to divert the communication over different carriers.

Even in this case the system can collect useful information about the attacker; such information can be used to envisage a new defensive strategy or simply to recognize the condition in a future occurrence.

4 Spectrum Sensing for SPD driven transmission and Trusted and dependable connectivity

In this chapter the main used techniques and algorithms presented in the open literature for spectrum sensing will be presented. It is important to note that this task is one of the most important to obtain an effective SPD driven transmission.

In fact, by sensing the surrounding environment it is possible to acquire the context awareness which is then used to define the optimal configuration for the system according to a given goal (e.g., according to SPD requirements). However, spectrum sensing is a complex task especially when real scenarios are considered.

In fact, sensed signals are ususally corrupted by channel impairments which can lead to an incorrect radio awareness and to a consequent erroneous system configuration. In particular, some architectures which allow improving the performances of spectrum sensing will be proposed in the following.

4.1 Algorithms for Spectrum Sensing

As has been pointed out in the previous sections, a Cognitive Radio has to be able to sense the environment over a wide portion of the spectrum and autonomously and dynamically adapt to it according to available resources and the defined SPD goals.

This task performed by Cognitive Radio is known as Spectrum Sensing [2], [3], [12]. Generally speaking, Spectrum Sensing in wireless communications is one of the most challenging tasks that a Cognitive Radio has to perform.

Depending on the required level of automation and self-management capabilities, Spectrum Sensing has to provide to the Cognitive Radio different information in order to predict the radio spectrum utilization.

For these reasons, in some applications, providing information only about the frequency usage would not be sufficient, and other characteristics about the portion of the spectrum under investigation have to be provided in order to predict the radio spectrum utilization (e.g. number of transmitted signals, carrier frequency, power, transmission technique, modulation, etc). In fact, prior knowledge about the transmitted signal and its parameters (e.g. carrier frequency, power, modulation, etc.) is usually not available.

Moreover, received signals are corrupted by channel distortions (e.g. severe multipath fading), and spread spectrum transmission techniques are often used in order to obtain a low probability of interception.

4.1.1 Signal processing techniques for spectrum sensing

In order to provide a fast and reliable spectrum sensing, different techniques have been proposed in the last decades [13], [14], [15], [16] for signal detection [14], automatic modulation classification [15], radio source localization [16], etc.

4.1.1.1 Energy detector based spectrum sensing

One of the most commonly used approach to detect the presence of transmissions is based on energy detector [13], also known as radiometer, that performs a measurement of the received energy in selected time and frequency ranges [13]. Such measurement is compared with a threshold which depends on the noise [10].

The presence of a signal is detected when the received energy is greater than an established threshold. Energy detector is widely used because of its low implementation, computational complexities and, in the

general case where no information regarding the signal to be detected is available, is known to be the most powerful test and can be considered as optimal.

On the other hand, energy detector exhibits several drawbacks [10], [17] which can limit its implementation in practical CR networks. In fact, the computation of the threshold used for signal detection is highly susceptible to unknown and varying noise level [14], resulting in poor performance in low Signal to Noise Ratio (SNR) environments [14].

Furthermore, it is not possible to distinguish among different primary users since energy detectors cannot discriminate among the sources of the received energy [18]. Finally, radiometers do not provide any additional information regarding the signal transmitted by the primary users [10][19] (e.g. transmission standard, modulation type, bandwidth, carrier frequency) which can be useful to predict spectrum usage by primary users [19], allowing to avoid harmful interference while increasing the capacity of CR networks [17].

4.1.1.2 Matched fileter based spectrum sensing

When the perfect knowledge of the transmitted waveform (e.g. bandwidth, modulation type and order, carrier frequency, pulse shape) [10], [18] is available, the optimum approach to signal detection in stationary Gaussian noise is based on matched filters [17]. Such a coherent detection requires relatively short observation time to achieve a given performance [10] with respect to the other techniques discussed in this section.

However, it is important to note that, in CR networks, the transmitted signal and its related characteristics are usually unknown or the available knowledge is not precise. In this case, the performances of the matched filter degrades quickly, leading to an undesirable missed detection of primary users [20]. Moreover, this approach is unsuitable for CR networks, where different transmission standards can be adopted by primary users [18].

As a matter of fact, in these cases, a CR terminal would require a dedicated matched filter for each signal that is expected to be present in the considered environment, leading to prohibitive implementation costs and complexity [18].

4.1.1.3 Feature detection based spectrum sensing

An alternative approach to spectrum sensing is based on feature detection [14], [18], [21], [22]. Such an approach allows to extract some features from the received signals by using advanced signal processing algorithms and it exploits them for detection and classification purposes [21], [22].

In the spectrum sensing context, a feature can be defined as an inherent characteristics which is unique for each class of signals [20] to be detected.

To perform signal detection some commonly used features are instantaneous amplitude, phase and frequency [15]. Among the different feature detection techniques which have been proposed in the open literature [14], [15], [23], an approach which has gained attention due to its satisfactory performances [14], [24], [25] is based on cyclo-stationary analysis, which allows to extract cyclic features [10], [14], [25], [26], [27].

Such an approach exploits the built-in periodicity [14] which modulated signals exhibit since they are usually coupled with spreading codes, cyclic prefixes, sine wave carriers, etc [17]. The modulated signals are said to be cyclo-stationary since their mean and autocorrelation functions exhibits periodicities, which can be used as features.

Such periodicities can be detected by evaluating a Spectral Correlation Function (SCF) [24], [25], also known as cyclic spectrum [14], which, furthermore, allows extracting additional information on the received signal which can be useful to improve the performance of the spectrum sensing [19].

One of the main benefits obtained by using cyclo-stationary analysis is that it allows an easy discrimination between noise and signals even in low SNR environments [14]. Moreover, such an approach allows distinguishing among different primary users since unique features can be extracted for the classes of signals of interest. In spite of these advantages, cyclic feature detection is computationally more complex than energy detection and can require a longer observation time than matched filters [12].

4.1.1.4 Waveform-based Sensing

Known patterns are usually utilized in wireless systems to assist synchronization, equalization or for other purposes [10], [25]. Such patterns include preambles, midambles, regularly transmitted pilot patterns, spreading sequences etc [14], [20], [25].

A preamble is a known sequence transmitted before each burst and a midamble is transmitted in the middle of a burst or slot. In the presence of a known pattern, sensing can be performed by correlating the received signal with a known copy of itself [10] , [25].

This method is only applicable to systems with known signal patterns, and it is termed as waveform-based sensing or coherent sensing [10]. Usually, waveform-based sensing outperforms energy detector based sensing in reliability and convergence time [10]. Furthermore, it is shown that the performance of the sensing algorithm increases as the length of the known signal pattern increases [10].

However, it can be applied if the patterns are known and the other nodes in the network are cooperative [10].

4.1.2 Signal Classification for spectrum sensing

Once the received signal is processed by applying one of the algorithm presented in the previous section, signal detection has to be performed in order to identify opportunities for secondary transmissions without causing harmful interference to primary users.

Moreover, in this contribution, signal classification of the detected primary signal into a given transmission standard is performed, since it may be useful to predict some spectrum occupancy patterns of the primary signal, which indeed may be exploited to increase the sensing performance of the CR network. This is usually done by applying well known pattern recognition methods to a processed sampled version of incoming signals [29]. In general, the design of a classifier concerns different aspects such as data acquisition and pre-processing, data representation, and decision making [29].

In CR applications data acquisition is represented by analog-to-digital conversion (ADC) of the electromagnetic signal perceived by the antenna, while the pre-processing is represented by the signal processing techniques presented in Section 4.1.1.

The data representation could be provided by some extracted features which can be then used for decision making which usually consists in assigning an input data (also known as pattern) to one of finite number of classes [30].

Among the approaches which can be used for classification, Neural Networks (NNs) and SVMs has recently gained attention for spectrum sensing purposes [31], [32]. One of the most important advantages

is that these tools can be easily applied to different classification problems, and usually do not require deep domain-specific knowledge to be successfully used [29].

Recently, there has been an explosive growth of researches about NNs resulting in a wide variety of approaches [33]. Among them, the most appreciated one is feed-forward NNs with supervised learning [33] which are widely used for solving classification tasks [33]. Although it has been shown that NNs are robust in the classification of noisy data, they suffer in providing general models which could result in an over-fitting of the data [33].

SVMs represent a novel approach to classification originated from the statistical learning theory developed by Vapnik [34], their success is due to the benefits with respect to other similar techniques, such as an intuitive geometric interpretation and the ability to always find the global minimum [33]. One of the most important features of an SVM is the possibility to obtain a more general model with respect to classical NNs [34].

This is obtained by exploiting the Structural Risk Minimization (SRM) method which has been shown to outperform the Empirical Risk Minimization (ERM) method applied in traditional NNs [34].

SVMs use a linear separating hyper-plane to design a classifier with a maximal margin. If the classes cannot be linearly separated in the input data space, a nonlinear transformation is applied to project the input data space in an higher dimensional space, allowing to calculate the optimal linear hyper-plane in the new space.

Due to its widespread applications, nowadays different efficient implementations of SVM are available in the open literature [35], [36] and only few decisions regarding some parameters and the architecture have to be addressed in order to provide satisfactory performances.

Finally, some works pointed out that SVMs require a long training time, i.e. the time needed to design an efficient classifier adjusting parameters and structure [33]. However, SVMs can be still applied to spectrum sensing since the design of the classifier can be done off-line exploiting some a priori measurements which can be used as training data.

4.2 Spectrum sensing limitations and challenges

Although advanced signal processing and pattern recognition techniques can ease the task of spectrum sensing several limitations and challenges remain, especially when real environments are considered [10], [18].

In fact, CR terminals have to detect any primary user's activity within a wide region corresponding to the coverage area of the primary network and the coverage area of the CR networks [18]. For this reason, a CR terminal needs a high detection sensitivity [18] which is a challenging requirement for wireless communications, especially when spread spectrum transmission techniques are used by primary users.

Furthermore, spectrum sensing is more complex in those frequency bands where primary users can adopt different transmission standards, e.g. Industrial, Scientific, and Medical (ISM) band. In this case, a CR terminal has to be able to identify the presence of primary users detecting different kinds of signals, each one characterized by its features, by using a single detector to limit hardware costs.

Finally, it is important to remark that in wireless communications the received signal is corrupted by multipath fading, shadowing, time varying effects, noise, etc. These phenomena can cause significant variations of the received signal strength and, thereby, it could be difficult to perform reliable spectrum sensing [18], [37].

This is of particular importance in CR networks, where a false detected opportunity, e.g. due to a sudden deep fade, can lead to an incorrect spectrum utilization, causing harmful interference to primary users [18], [37].

As a final remark, in order to efficiently utilize the available radio resources, the duration and periodicity of the spectrum sensing phase have to be minimized. In fact, the opportunities have often a limited duration and CR terminals usually cannot exploit them [10], [18], while performing spectrum sensing.

4.3 Architectures for spectrum sensing

In this section, the main classes of spectrum sensing architectures will be shown. In particular, stand-alone single antenna, cooperative, and multiple antenna architectures will be considered (see Figure 4.1).

One of the most simple and widespread architectures is based on a standalone single antenna terminal. In this case the CR terminal, equipped with a single antenna, acts autonomously to identify the signals transmitted by the primary users on the observed frequency band [17].

The phases of the spectrum sensing process for this simple architecture are four and can be denoted as sampling, processing, information reduction and classification, as shown in Figure 4.1(a). It is important to remark that, although similar architectures have been proposed in literature [21], [22], no information reduction phase is performed.

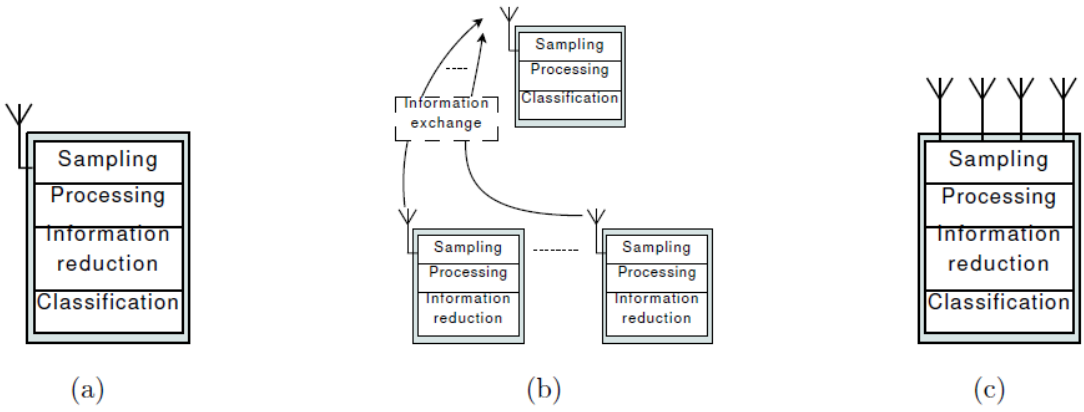


Figure 4.1 – Architectures for spectrum sensing: (a) stand-alone single-antenna; (b) cooperative terminals; (c) multiple antenna terminal

Let us analyze in detail each phase. The CR terminal exploits the single antenna to collect the signals radiated by primary transmitters. The amount of time employed for the signal collection is the so-called observation time.

This quantity should be as short as possible [18] in order to maximize the exploitation of the detected opportunity [10]. The received signal is sampled and then processed: as shown in Section 4.1.1, different advanced signal processing algorithms can be used, according to the available knowledge of the primary signals to be identified.

As an example, feature detection based techniques can be used in order to extract the unique characteristics of the different signals which can then be used for classification purposes.

To simplify the problem, decreasing the complexity of the following classification phase, and shortening the global elapsing time, the information contained in the highlighted characteristics can be reduced. As

an example, classical eigenvalue method for linear feature reduction [38], used in pattern recognition, can be applied in order to reduce the problem complexity.

Once the processing and the information reduction phases are performed, and the differences among signals are pointed out, a classification phase is required to discriminate among the signals transmitted by primary users. Different techniques, presented in Section 4.1.2, can be used in order to obtain a precise classification phase. As an example SVM [33], [35], [36] is a well-known classifiers which can be used for different problems and applications.

Despite the simplicity of the stand-alone single antenna architecture makes it attractive from an implementation point of view, it suffers in multipath and shadowing environments [20], [39] where the deep and fast fades of the received signal strength and the hidden node problem can lead to an incorrect spectrum utilization [10], [37]. In order to mitigate such drawbacks, a longer observation time can allow to achieve satisfactory performances, but such a solution is not exploited in practice since fast opportunity detection is desirable in practical CR networks [10].

To overcome the disadvantages of the stand-alone single antenna architecture, cooperative and multiple antenna architectures can be proposed [10], [20]. In particular, while both cooperative and multiple antenna system can be employed to mitigate multipath fading, just cooperative approach can be used to limit shadowing effects.

Multipath (fast) fading, i.e. deep and fast fades of the received signal strength, is the most characteristic propagation phenomenon in multipath environments. However, its degrading effects can be overcome by exploiting the spatial diversity due to the different positions of the CR terminals or of the several receiving antennas, in cooperative and multiple antenna systems, respectively.

In fact, the antennas separated one wavelength or more are expected to obtain uncorrelated signals [40], [41] and thereby each antenna receives a signal corrupted by an independent multipath channel providing the required diversity [39], which can be exploited for improving radio awareness [42].

As opposed to fast fading, which is a short-time scale phenomenon, the so called shadowing or slow fading, a long-time scale propagation phenomenon, can also be considered. This effect occurs when the transmitted signal experience random variation due to blockage from objects in the signal path, giving rise to random variations of a received power at a given distance [39].

This phenomenon can cause the undesiderable hidden node problem [10], [37] that can be still overcome by means of spatial diversity. However, in this case, the receiving antennas need to be separated by

much more than one wavelength since the shadowing process is frequently correlated over larger distances, in the order of tenths of meters or more. This means that the multiple antenna architecture would not be able to overcome the hidden node problem since all received signal versions would be affected by the same level of shadowing attenuation.

On the contrary, the cooperative architecture may be able to overcome the hidden node problem if the cooperating CRs are apart enough to receive sufficiently uncorrelated versions of the same primary signal.

As regards the other aspects, firstly let us consider the cooperative architecture where the CR terminals form a distributed network sharing the collected information in order to improve the performances of the spectrum sensing phase [42].

Different strategies of cooperation and network topologies can be implemented. In this work, a centralized network will be considered. In particular, the considered architecture is composed by a set of cooperative single antenna terminals, as shown in Figure 4.1(b), which individually sense the channel, sample and process the received signal, and finally send the collected information to a fusion center, usually represented by a predefined terminal belonging to the network with enhanced signal processing capabilities.

It aggregates the received local observations [42] for identifying the signals transmitted by primary users.
Among the advantages of such an architecture, it is important to remark that it allows not only a performance improvement but also is well suited for IEEE 802.22 WRAN [12], where a base station can act as fusion center [37].

As regards the costs, it is possible to highlight that, on the one hand, the cooperative CR terminals can achieve the same performances of a standalone CR terminal by using less performing and cheaper hardware [37]. On the other hand, the increase of the number of terminals leads to a consequent rise in costs. Moreover, the information forwarded to the fusion center implies the introduction of a dedicated control channel (not always available in CR contexts), and a consequent coarse synchronization, to avoid a modification of the electromagnetic environment during the spectrum sensing phase.

Since a control channel may not be available in practical CR applications, a multiple antenna architecture can be considered as an alternative solution for providing the useful spatial diversity.
In such an architecture, the CR terminal receiving antennas are thought as an antenna array with a digital beamforming receiving network, as shown in Figure 4.1(c).

This strategy, that is similar to a distributed system architecture with an ideal control channel (i.e. no transmission delay and channel distortions), exploits the complexity of the environment, as happens for multiple-input multiple-output systems [39].

Multiple antenna architectures do not require a control channel and allow to take advantage from the spatial diversity [39] also for the opportunity exploitation, by managing the radiation pattern so as to mitigate the interference with primary users [9].
However, the previously advantages are paid in terms of an increase of the hardware costs due to the presence of several receiving antennas and to the higher processing capabilities required for real-time aggregation of the signals gathered by each antenna.

Note that essentially the same processing chain, shown in Figure 4.1(a), can be applied to all the considered architectures. However, there are some differences. The most evident one is the introduction of an information exchange phase, if the cooperative architecture is considered.

4.4 Security problems during spectrum sensing

Although cooperative or distributed sensing is proposed to identify unused resources, unfortunately, there are several security issues which need to be investigated in order to obtain a SPD spectrum sensing. One of the most significant threats is the user emulation (UE) attack.

In particular, in the cognitive radio context, it is supposed that user at the same level in the hierarchy (secondary user) can share the radio resource, but if another user (primary user) which is in a higher level of the hierarchy needs the resource, the secondary users have to vacate it. In a UE attack, a malicious secondary user attempts to gain priority over other secondary users by transmitting signals that emulate the characteristics of a PU's signals.

The potential impact of a UE depends on the legitimate secondary users' ability to distinguish attacker's signals from actual PU signals while conducting spectrum sensing. Note that this attack is Energy detection is unable to distinguish primary signals and secondary signals and thus particularly vulnerable to UE attacks.

Another possible threat is known as spectrum sensing data falsification. In this case, a malicious user sends fake local sensing results to the fusion centre (if any, otherwise to the other cooperative users) so it can take a wrong decision about resource allocation. In this case an authentication mechanism is

required to avoid sensing data falsification. In Figure 3.1 – the user emulation and spectrum sensing data falsification are reported.

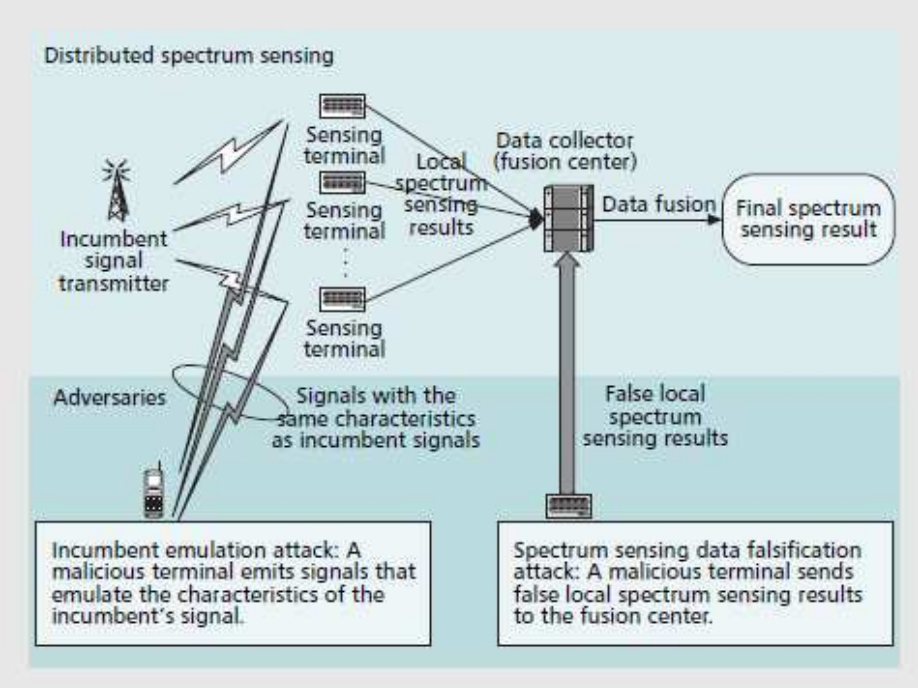


Figure 4.2 – Security threats during distributed or cooperative spectrum sensing [37]

4.4.1 User emulation attack

In this case, the malicious user emulates the behaviour of another user trying to get privileges in accessing the available resources or trying to set up a communication with other users to steal some information.

In particular, an incumbent malicious user can acquire privileges to transmit in a given frequency band, avoiding to other fair users (i.e., with rights in that frequency band) to fully exploit the resources since they have to be shared with other, not allowed, users. Moreover, once the privileges to transmit is acquired by an ill-intentioned user, it may try to set up a communication with fair users and consequently significant SPD problems arise [37].

As an example, an user emulation attack is shown in the lower left corner of **Error! Reference source not found.**. It is important to note that, it is possible for an adversary to dynamically modify the radio

software of a CR to properly set the transmitted waveform (e.g., carrier frequency, bandwidht, power) so that it resemble the one of the fair users in the considered network.
The potential impact of an user emulation attack depends on the capabilities of the other users to distinguish the signal of the malicious user from the signal of the honest and fair users. In the following, two existing spectrum sensing techniques, presented in Section 4.1.1, are briefly reported and the reasons why they may be vulnerable to the descibed attack [37].

One of the most used algorithms for spectrum sensing is based on energy detection. An energy detector, also known as radiometer [13], can detect the presence of a signal in a given environmet if the received energy level is over a given threshold. It is omportant to stress that this kind of detection does not allow to distinguish among signals, but only to detect the users' activity [13], [14], [37]. Then, it is not possible to identify malicious user.

However, an improved scheme, proposed in [46], suggest the use of quite periods, i.e., in order to ease the spectrum sensing task to detect malicious users, other users remain silent for a given period. If the quite period is respected by all the fair users in the networks, detecting ill-intentioned users become straightforward.

In fact, by using energy detection based spectrum sensing, any terminal leading to a signal energy level over a given threshold during quite period can be considered as malicious.
Another approach to spectrum sensing is based on signal feature detection [4], [10], [14], [25], [32], [37], [42] or matched filter detection [10], [17], [18], [20], [37] to detect signal characteristic of a fake user. It is important to note that, relying on signal feature detection can not be secure and reliable to distinguish among malicious and fair signals.

In fact, the attacker can sniff some transmissions among fair users and then replay the signals that were previously recorded. In this case, signal feature detection will falsely identify the signal as transmitted by a fair user, while, actually, it is not.

Moreover, in [37], it has been proved that user emulation attacks can lead to an undesirable and drastical decrease of the available resources allocated to fair users. It is now aboundantly clear that it is necessary to mitigate the disruptive effects of this attack for trusted and dependable connectivity. To this end, in the next Section 4.4.2 some procedures to deal with these problems are presented.

4.4.2 Defending against user emulation attack

In order to defend against user emulation attack, it is necessary to develop and adopt a secure and dependable technique for verifying the authenticity of the users which need to communicate within the network. One of the simplest approach is to provide the fair users with a signature. Otherwise, it is possible to implement and employ an authentication protocol between the transmitter and a SPD verifier.
In this context, in order to improve the SPD, it is proposed to add other systems for verifying the authenticity [37].

In particular, in [47], it is supposed that the users are in fixed positions or can move in with low speed. In this case, the location of the users can be used as a characteristic to identify illegal access to the network. However, it is imporant to note that malicious users that are close to the fair user cannot be easily identified [37].

To overcome this problem, in [37], [47], it is proposed another distinguish property. In particular, it is assumed that legal users use a fixed transmitted power, within a given range. Therefore, a malicious user can be identified by using a combination of the location and of the received signal power level.

Of corse, to use only this property to identify illegal access could not be sufficient, since received signal power can vary, even significantly, in wireless channels, where multipath fading, shadowing, pathloss, etc. usually corrupt the transmitted signals. However, there are different techniques which can be used to reliable estimate the received signal power. These techniques are presented in [48], [49] for both Additive White Gaussian Noise (AWGN) channel and multipath channel.

However, the most difficult task is to estimate or verify the location of the origin of a transmitted signal. In fact, it is usually assumed that the ill-intentioned user is not collaborative in estimating his position and it not interacts with the location estimation or verification scheme. There are different techniques and algorithms which can be used to deal with this problem. Here, the most used techniques [50], [51] are reported.

4.4.2.1 Distance Ratio Test

One of the techniques is the Distance Ratio Test (DRT). It exploits the received signal strength (RSS) measurements obtained from a pair of location verifiers (LVs) to verify the location of the transmitter. A LV is defined as a dedicated network device (e.g., a Base Station or a fair user with enhanced processing capabilities) able to perform location verification. Single LV devices form a network and communicate each other. For SPD reasons it is assumed that the data exchange is secure by using a security protocol [50], [52].

This appraoch exploits the strong correlation between the RSS and the length of the active wireless link. In particular, the RSS measurements at two different LVs correlate with their resspective distance from the location of the source. Note that the RSS depends on some parameters wich can be adjusted at the transmitter such as, transmitted power, antenna gain, etc [50].

However, if the two considered LVs employ identical radio receivers, and if a sufficient similar to reality radio propagation model is assumed to be known, then it is possible to state that the ratio between their RSS measurements only depends on the ratio between their respective distances to the location of the transmitter [37].

Note that, it is possible to evaluate the expected ratio if the respective distances between each LV and the transmitter by using the location information of the two LVs and the assumed position of the transmitter [37].

This ratio is compared with the ratio derived from RSS measurements taken from each LV. If the expected value and the measured value are sufficiently close (to a predefined threshold), the transmitter is considered legal and passes the location verification; otherwise it fails the verification [37].

One of the most important drawbacks of the DRT approach is that its efficacy is influenced by the radio propagation model. In fact, it is affected by various environmental variables [37].

Different propagation environments may require the use of different parameters leading to a totally different propagation model. To address such issues, significant changes to the aforementioned DRT technique are required.

4.4.2.2 Distance Different Test

Another technique which can be used to address the problem of location verification is the so called Distance Difference Test (DDT) [37]. It is based on the fact that when a signal is transmitted from a source towards two different receiver (i.e., two LVs in the case of interest), the received signal is expected to be perceived with two different phase shifts [37]. These different shifts are derived from the different distances [37].

The phase difference can be translated into a time difference that in turn can be translated into a distance difference [37]. One can calculate the expected difference of the respective distances between each LV

and the transmitter by using the location information of the two LVs and the assumed position of the transmitter [37]. This expected difference is compared with the measured difference to determine the authenticity of the signal [37]. If the two values are sufficiently close, the transmitter is considered legal and passes the location verification; otherwise it fails the verification [37].

Note that the DDT technique is not affected by the drawbacks of the DRT technique (i.e., it does not require a precise propagation model). However, the DDT could require strict synchronization among the LVs which is not easy to implement [37], [50].

4.4.2.3 Other approaches under investigation

When the ill-intentioned are mobile and have low transmission power users obtain an effective defense against user emulation attacks is more challenging.

One possible solution [37], [51] could be to exploit the Radio Environment Map (REM). It is an integrated Data Base (DB) which consists of a comprehensive collection of information for the whole networks, including the active legal radio device, the locations, the transmission parameters, etc.

This DB is located in the LV and it is made reliable, secure and dependable accessible to LVs. So, it is possible to verify an incumbent transmitter by comparing its observed location and activities with those stored in the REM. However, more research is still to be done to make such a solution practical.

4.4.3 Spectrum sensing data falsification

Although cooperative and distributed spectrum sensing can allow to improve the performance of the detection of active users, there are some security threats which need to be addressed to guarantee a SPD driven transmission and a trusted and dependable connectivity.

In particular, the user emulation attack (see Section 0 and Section 4.4.2 for details) and the spectrum sensing data falsification threats are the most important. In this section the attention is focused on the latter. It consists of a transmission by a malicious user of false spectrum sensing data to the fusion center.

In particular, an attacker can send fake local spectrum sensing results to the data collector with the aim to cause in the data collector a wrong spectrum sensing decision and a consequent incorrect resource allocation to the users. Note that this kind of attack is reported in the lower right corner of **Error! Reference source not found.** and is usually known as spectrum sensing data falsification (SSDF) attack.

In order to guarantee a sufficient level of SPD in the case of SSDF attack, it is necessary that the data fusion technique used in the data collector during cooperative spectrum sensing is robust against fraudulent local spectrum sensing results reported by malicious users.

In spite of the numerous techniques for data fusion which have been recently proposed, none address this problem. In particular, in the following the attention is focused on three commonly used data fusion techniques proposed for traditional cooperative spectrum sensing. Each algorithm is presented and its vulnerability to SSDF attacks is shown.

For the sake of simplicity, the cooperative spectrum sensing problem is modeled as a parallel fusion network, as shown in **Error! Reference source not found.**. In particular, a parallel fusion network with data fusion [4] is considered. In this case, a set of N cooperative cognitive radios cri share the same radio environment. Each cognitive radio performs spectrum sensing by one of the techniques proposed in Section 4.1.1 according to its computational capability.

Then, it sends the output of the spectrum sensing task to a data fusion center, which provides a “global” spectrum sensing decision based on gathered data [4]. It is necessary to remark that in this context, different solutions can be proposed depending on the level of cooperation among cognitive radios [4].

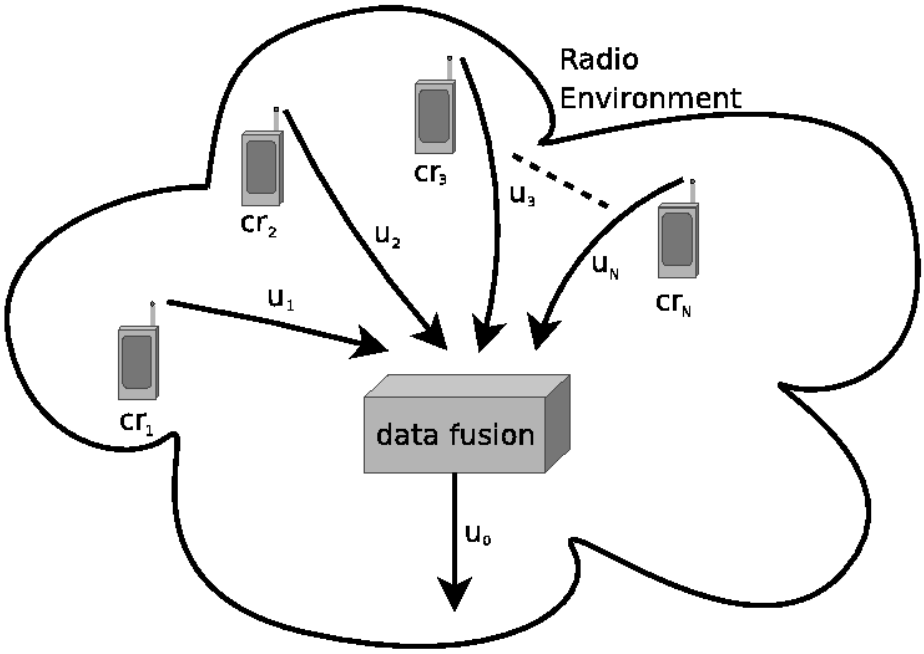


Figure 4.3 – Parallel fusion network with fusion [4]

An example of distributed detection with fusion is shown in **Error! Reference source not found.** [4]. In the rest of the section the following notation is used.

The observation of the radio spectrum used as input to the spectrum sensing phase at the cognitive radio cri is represented with y, the local spectrum sensing result is represented with ui that cri sends to the data fusion center.

The output u is the final sensing result, which is a binary variable. A one denotes the presence of an user's signal, and a zero denotes its absence. To simplify the discussion, the following description assumes that spectrum sensing is performed in a single band, and each u_i is binary too.

4.4.3.1 Decision fusion

The fusion center receives the local decision u_i and applies a fusion rule to combine them [54]

$$T = \sum_{i=1}^{N} u_i = \begin{cases} u = 0 & if \quad T < k \\ u = 1 & otherwise \end{cases}$$

where u=0 indicates that the primary users are absent, and u=1 indicates that the primary users are present.

Note that the fusion rule reported above represents the k out of N fusion rule and indicates that the global decision u = 1 if at least k terminals over N decide for the presence of the primary users. The OR and the AND fusion rules represent a special case of the k out of N fusion rule. In fact, for k = 1 the fusion rule coincides with the OR fusion rule, while for k = N it coincides with the AND fusion rule [54].

It is important to remark that the OR fusion rule is much conservative in using the licensed resources with respect to the AND fusion rule [54]. In fact, the OR fusion rule does not allow secondary transmissions even if a single secondary terminal in the CR network detects the primary users' activity.

On the contrary, the AND fusion rule does not allow secondary transmissions only if all the secondary terminals in the CR network detect the primary users' activity. Finally, note that the spectrum sensing data to be sent at the fusion center to make the global decision u are the local decisions $u_i \in \{0,1\}$, i.e. a bit in the binary hypotheses testing problem. In practice, the transmission of the local decisions ui to the fusion center can be affected by channel impairments [54].

However, Adaptive Modulation and Coding (AMC) techniques [39] can mitigate this issue, especially if the amount of data to be shared is limited [54].

Because interference among users derived by incorrect resource allocation should be minimized, usually a conservative strategy is preferred setting a threshold k value of one. In this case, even if a band is free, as long as there is one cri that erroneously reports u_i = 1, the final result will be busy, causing a false alarm. If an SSDF attacker exploits this and always reports one as its local spectrum sensing result, then the final result always will be busy [37].

To prevent such a scenario, one can increase the threshold k value [37]. However, increasing the threshold value has the downside of increasing the miss detection probability [37]. Moreover, increasing the threshold k is ineffective in decreasing the false alarm probability when there are multiple attackers [37].

4.4.3.2 Bayesian detection

This technique for combining the spectrum sensing data received by each node of the network requires the knowledge of a priori conditional probabilities of ui's when u is zero or one [37].

Moreover, it is necessary to know the a priori probabilities of u. Four cases must be considered [37], [46]:
u = 0 when a given band is free;
u = 0 when the band is busy;
u = 1 when the band is free;
and u = 1 when the band is busy.

Among the four reported cases, two decisions are correct, and the other two are wrong. The two correct ones are allocated with small costs, and the wrong ones are associated with large costs [37], [46]. The miss detection case is the least desired scenario and therefore is assigned to the largest cost [37], [46]. The overall cost is the sum of the four costs weighted by the probabilities of the corresponding cases [37], [46].

Bayesian detection outputs a final spectrum sensing result that minimizes the overall cost [37], [46]. When a network is under SSDF attacks, the values of the a priori conditional probabilities of the ui's are not trustworthy [37], [46]. As a result, Bayesian detection is no longer optimal in terms of minimizing the overall cost [37], [46].

5 Physical layer Techniques enabling SPD driven transmissions and Trusted and dependable connectivity

Cognitive radios try to optimize the system configuration by introducing the dynamic usage of available resources. It can be defined as an intelligent wireless system that is aware of its surrounding environment through sensing and measurements; a system that uses its gained experience to plan future actions and adapt to improve the overall communication quality and meet user needs.

One main aspect of cognitive radio is its ability to dynamically exploit available resources to provide new ways of communication. Hence, cognitive radio should have the ability to sense and be aware of its operational environment, and dynamically adjust its radio operating parameters accordingly. For cognitive radios to achieve this objective, the Physical Layer (PHY) needs to be highly flexible and adaptable.

Spectrum underlay: In spectrum underlay, secondary users are allowed to transmit their data in the licensed spectrum band when primary users are also transmitting. The interference temperature model is imposed on secondary users' transmission power so that the interference at a primary user's receiver is within the interference temperature limit and primary users can deliver their packet to the receiver successfully.

Spread spectrum techniques are usually adopted by secondary users to fully utilize the wide range of spectrum. However, due to the constraints on transmission power, secondary users can only achieve short-range communication. If primary users transmit data all the time in a constant mode, spectrum underlay does not require secondary users to perform spectrum detection to find available spectrum bands.

Spectrum overlay: Spectrum overlay is also referred to as opportunistic spectrum access. Unlike spectrum underlay, secondary users in spectrum overlay will only use the licensed spectrum when primary users are not transmitting, so there is no interference temperature limit imposed on secondary users' transmission. Instead, secondary users need to sense the licensed frequency band and detect the spectrum white space, in order to avoid harmful interference to primary users.

5.1 Ultra Wide Band (UWB)

When the wireless systems that are potential candidates for cognitive radio are considered, UWB seems to be one of the tempting choices because it has an inherent potential to fulfil some of the key cognitive

radio requirements [44]. However, it is worth to stress that a cognitive radio might have the ability to synthesize and process various waveforms and wireless technologies [44].

Under the current regulation, UWB is a promising technology for future short and medium range wireless communication networks with a variety of throughput options including very high data rates [44]. UWB's most significant property is that it can coexist in the same temporal, spatial, and spectral domains with other licensed/unlicensed radios because it is an underlay system [44].

Other tempting features of UWB include that it has a multi-dimensional flexibility involving adaptable pulse shape, bandwidth, data rate, and transmit power [44]. On top of these, UWB has a low-power consumption, and it allows significantly low complexity transceivers leading to a limited system cost [44]. It also has an advanced multipath resolution capability.

Another very important feature of UWB is providing secure communications [44]. It is very hard to detect UWB transmission as its power spectrum is embedded into the noise floor [44].

This feature introduces very secure transmission in addition to other possible higher layer encryption techniques [44]. The attractiveness of UWB for cognitive radio is not limited to the inherent attributes of this technology [44]. UWB offers some exceptional uses that can add a number of extra intellective features to cognitive systems [44].

These special uses are brought by the high multipath resolution property, which enables UWB to act as accurate radar, ranging, and positioning system [44]. Examples of specific UWB features include sensing the physical environment to enable situation awareness, providing geographical location information, and specifying the mobile communication parameters when one or more users are nomadic [44].

5.2 Orthogonal Frequency Division Multiplexing (OFDM)

The cognitive engine is responsible for making the intelligent decisions and configuring the radio and PHY parameters [45].
The spectral opportunities are identified by the decision unit based on the information from policy engine as well as local and network spectrum sensing data [45].

The policy engine provides information to the cognitive engine concerning the current policies to be considered depending on the system location [45]. This will ensure that the cognitive radio will not use illegal waveforms or breach any policies. On the other hand, the local spectrum sensing unit process the

spectrum information and identify licensed users accessing the spectrum, their signal specifications such as their bandwidth and power level, and detect spectrum opportunities that can be exploited by cognitive radios [45].

Once the required information is available, the decision unit can make a conclusion on the best course of action for the system [45]. The decision includes choosing the appropriate channel coding, modulation, operation frequencies, and bandwidth [45].

At this stage, OFDM technology gets the upper hand over other similar transmission technologies with its adaptive features and great flexibility [45]. By only changing the configuration parameters of OFDM and radio, the cognitive system can communicate with various radio access technologies in the environment, or it can optimize the transmission depending on the environmental characteristics [45].

OFDM benefits:
Since it uses FFT/IFFT during demodulation/modulation, these transformations can be used for Sensing and awareness purposes
It is flexible and can allow spectrum shaping (i.e., fitting to the available resource)
It is adaptive (i.e., bandwidth, bit loading, symbol time, etc.)
Well suited to be employed with multiple antenna technologies
Well suited to be used also as multiple access scheme (i.e., OFDMA)
Interoperability with legacy wireless communication systems (for example, IEEE 802.11a/g, IEEE 802.16e, DVB-T/H, IEEE 802.15.3a, etc.)
OFDM challenges:
PAPR and synchronization
To have effective spectrum shaping it is necessary to design innovative filters to avoid out-of-band power emissions
To have effective spectrum shaping it is necessary to exchange the values of the parameters to be used to design the transmitted waveform
Mutual Interference in the case of OFDMA

6 RF Parameters

Providing long range, high throughput, high efficiency, and small dimensions at the same time implies a tradeoff among several factors, particularly while designing portable devices to be used in complex environments rich of obstacles like urban areas, noisy and crowded.

Low frequencies (HF, VHF) assure very long range (>100 km) even in non-LOS condition but with very narrow bandwidth (kHz). Antennas are huge and exhibit low efficiency. RF power generation is very cheap but circuits are big.

On the other side high frequencies (EHF) assure large bandwidth (>100 MHz) but short range (<10 km); antennas are very short (cm); propagation is purely optical. RF power generation is expensive.

Experience shows that a reasonable trade-off is to use low portion of UHF spectrum, i.e. 200 ÷ 500 MHz range.

Propagation in that range is not yet fully optical, so limited extension to non-LOS is practicable, permitting additional coverage.

Rain attenuation is negligible and attenuation by natural obstacles like trees is limited, allowing a significant range even in forests (~500 m).

Channel can be enlarged up to a few MHz, giving a reasonable throughput for multiuser high data rate communications.

Efficiency of RF active devices is pretty good and antenna dimensions can be kept limited (~10 ÷ 20 cm) without heavy loss of efficiency.

A portable terminal suitable for our purposes can be designed with dimensions comparable to first generation cellular phone using standard components.

Subsequent improvement might be obtained designing dedicated components (ASICs).

There is evidence that a communication range of 2 km in LOS is satisfactory for almost any mobile application.

RF power around 5 W is sufficient to provide coverage in excess of 2 km with omni-directional antenna (whip type).

The capability to implement multi-hop relaying allows range extension up to 10 km and more.

Provision for terminals placed in fixed, elevated locations further extends coverage.

Extension of RF band down to VHF provides additional capability in term of coverage and range, and could be exploited in extreme conditions.

A low rate channel in VHF could be useful to provide connection when the wideband channel is not available due to extreme environmental conditions (tunnels, mines, intra-building) or if under attack.

Extension to VHF is cheap with current technology of standard components.

Usable spectrum will be the range 30 ÷ 500 MHz.

7 Cognitive Radio Node Simulator

The implemented Cognitive Radio Node is able to receive radio parameters from moving hosts and automatically detect possible threats.

The internal architecture of the Node learns typical safe environments features thus detecting the presence of external attackers by analysing radio parameters.

In a considered scenario, the cognitive node always updates the radio parameters (SNR, BER and Transmitter Power, PTX) for the self-awareness purposes.

There are some specific provisions considered to design this kind of simulator used for the Security, Privacy and Dependability (SPD) in the context of integrated and interoperating heterogeneous applications.

When an agent enters the scene, the cognitive node becomes aware of the radio parameters of the agent either by using the spectrum sensing technique or from a direct communication from the agent itself. In this way the node can update its radio information for using the radio resources efficiently and securely.

The cognitive node has an internal knowledge of all the radio parameters which would be considered in the selected environment and their respective variation models.

The node knows itself from a configuration database what frequencies are used by which agent and which frequencies are free to use. If a new agent enters in the scene while continuing communication, the cognitive node sense the radio parameters of the agent and is able to modify and adapt agents radio parameters when necessary.

In the presence of a jammer of specific frequency in a cluster, the cognitive node sends a message to the agents to adjust the radio parameters properly, i.e., by changing either the frequency or the transmission power (spread spectrum or noise based data transmission of signals).

An image of the simulator in consideration is shown in the following figure. In the scene, there are two entities with both active communication on different frequencies. Area affected by the movement of

such entities are three jammer that inhibit different frequencies and presents a range of different from each other.

Moving agents in the scene and the presence of jammers are dynamically created through a specific simulator that was built to this aim. The simulator sends to the cognitive node the positioning data, namely the trajectories of the agents (like a tracker) and radio data on the situation.

More specifically, each agent is controlled by the cognitive mobile node, considered as an entity, after the registration process in the area under observation, periodically sends information on the quality of communication.

Figure 7.1 – Considered scene of the simulator (Jammer, First Agent and Second Agent in the scene)

In the simulator there are six (06) types of interaction regarded between two different agents (guard/intruder), in particular:

a) ‘Agents in Motion’: Two entities with communication capabilities moving in the scene without interacting each other. One may be the network and the second a new communication node.
b) ‘Guard-Intruder Agents’: one or more communication nodes belonging to the network are the guard and another is the intruder. When the guard observe an intruder inside its region under control, the guard starts the procedures to identify and localize the menace to counteract the action of the intruder and as a consequence, the intruder try to overcome the countermeasures quickly.
c) ‘Meeting Agents’: Two communications entities meet/gather inside the scene and after meeting they link together.
d) ‘Leave & Meet Agents’: The two communications entities link inside the scene and leave the area individually.
e) ‘Running Agents’: Two communications entities running inside the scene but without interact each other.
f) ‘Run & Walk Agents’: One is running inside the area under consideration and the other is walking but without interact each other.

8 Embedded system based on multicore platform

An embedded system based on a multicore architecture was developed, in order to validate the results of the current studies. The platform starts from the results of a Finmeccanica corporate project named OMBRA (Open Multicore Based Reliable Architecture).

The Hardware (OMBRA v2-pShield) was adapted for the mentioned purpose, basing on the requirements that have been identified for the validation of the new cognitive algorithm studied for the SPD of SDR network.
The target is to identify and validate some functionalities of “automatic recognition of danger situations”, that in future will be developed and added to the products.

The architecture adopts different cores (CPU-ARM and DSP), instead of the replication of the same core, allowing better implementation of heterogeneous algorithms.

Another important feature is the high computational power versus low energy consumption.

The provider of the processor, Texas Instruments, inserted the multicore processor in the commercial, industrial and space lines, covering various applications of the electronic companies.

The board is a very small factor, very low power, SOM with a Netbook computational power to be used as a standard component within electronic companies projects where a standard CPU module (Linux or WinCE) is required, supporting cognitive algorithms.

The Board is based on ARM CortexA8@1Ghz with up to 1 GB LPDDR ram, wireless connections and includes a FPGA to allow the project to be customized by the user.

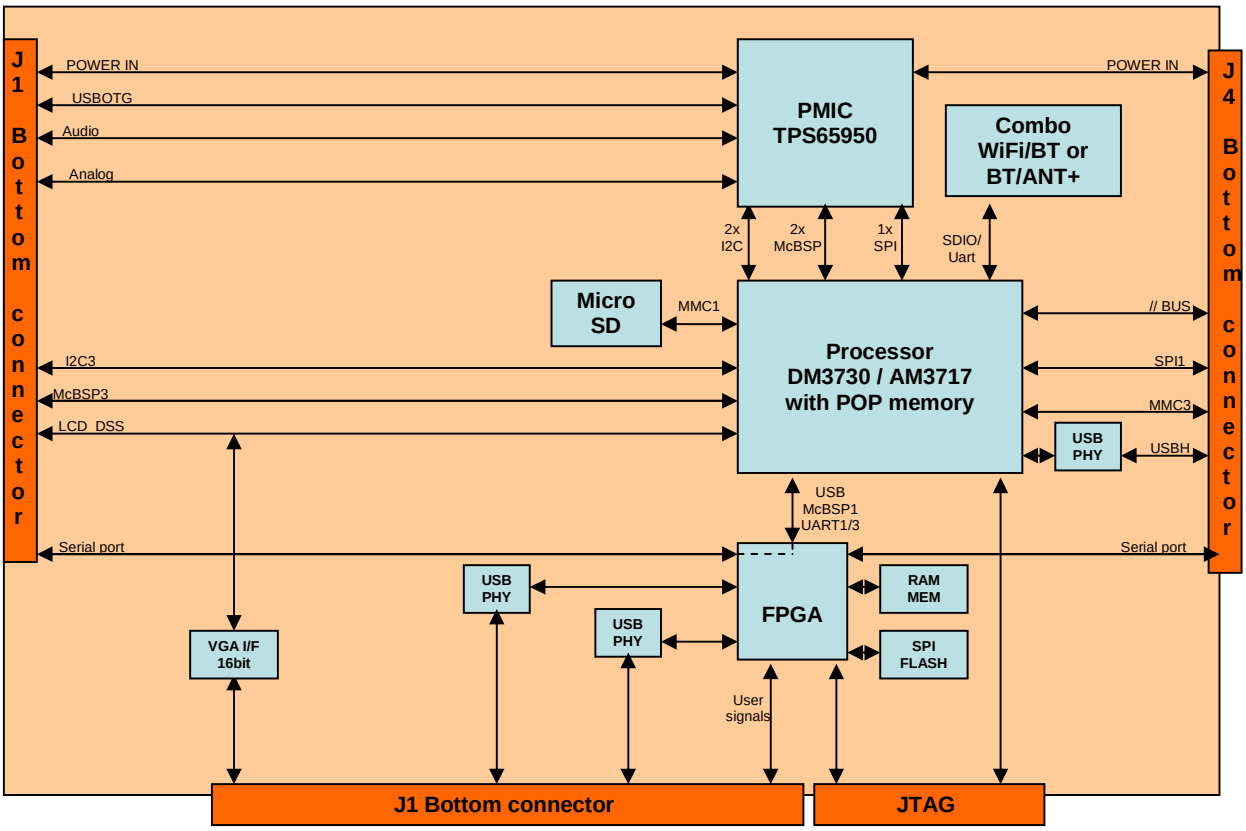


Figure 8.1 – Block Diagram

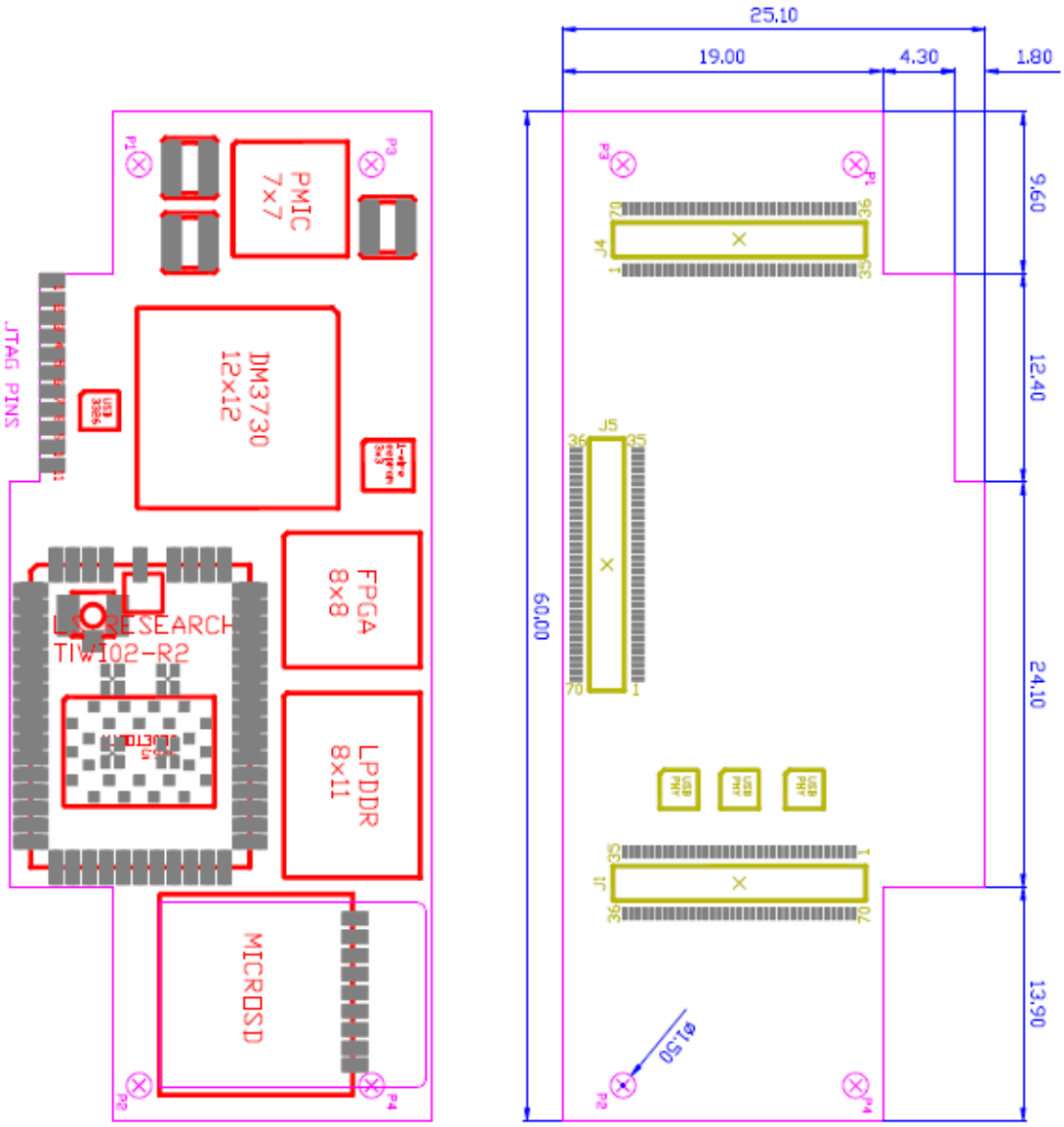


Figure 8.2 – LAYOUT and DIMENSIONS (draft)

DESCRIPTION	Full version	Lite Version
Processor	Ti DM3730	Ti AM3717
ARM CortexA8 processor speed	1Ghz	1Ghz
DSP	TMS320C64+	-
DSP processor speed	800Mhz	-
Ram Memory (LpDDR)	1024 Mbyte	512 Mbyte
Flash Disk	On uSD card up to 32GB	On uSD card up to 32GB
Video 3D acceleration	PowerVR SGX530	PowerVR SGX530
Wireless connection WiFi	IEEE 802.11 b/g/n (*)	
Wireless connection Bluetooth	2.1+ EDR class 1.5	2.1+ EDR class 1.5
Wireless connection PAN	ANT+ (*)	ANT+ (option)
Wireless Bluetooth/WiFi/ANT+	Unified u.Fl connector	Unified u.Fl connector
USB 2.0 OTG	1 connected to ARM (HS,FS,LS)	1 connected to ARM (HS,FS,LS)
USB 2.0 HOST	1 connected to ARM (HS only)	1 connected to ARM (HS only)
USB 1.1 HOST	connected to FPGA (FS only)	2 connected to FPGA (FS only)
USB 1.1 HOST/DEVICE sw configurable	connected to FPGA (FS, LS)	2 connected to FPGA (FS,LS)
Audio Stereo	Line-in and Line-out	Line-in and Line-out
Video VGA	16 bit (VGA and XGA)	16 bit (VGA and XGA)
Video Digital connection	DSS 24 bit 1v8 levels	DSS 24 bit 1v8 levels
FPGA	Xilinx Spartan6 (XC6SLX16-2CPG196I)	Xilinx Spartan6 (XC6SLX16-2CPG196I)
FPGA pins available for the user	11 (3v3 IO-level) + 20 (1v8 IO-level)	11 (3v3 IO-level) + 20 (1v8 IO-level)
Debug connection	JTAG both for processor and FPGA	JTAG both for processor and FPGA
Power Supply Range	3.2..4.2 Vcc, 2.5W	3.2..4.2 Vcc, 2W
Temperature range (components)	-40..+55 C	-20..+55 C

(*) the two options are alternative

Figure 8.3 – table of features

8.1 Connectors

The board has 3 expansions connectors J1, J4 and J5 (70 pin Series AVX5602) , to be used for connecting to the carrier board, plus a 4th board sided connector hosting JTAG.

The board can be delivered in two different versions, with or without J5 populated.

In the J5 populated version, the J1/J4 connections are mechanical and pin-out compatible with commercial Gumstix board
In the J5 not populated version J1 and J4 have custom variations to the commercial pinout.

J1 expansion connector

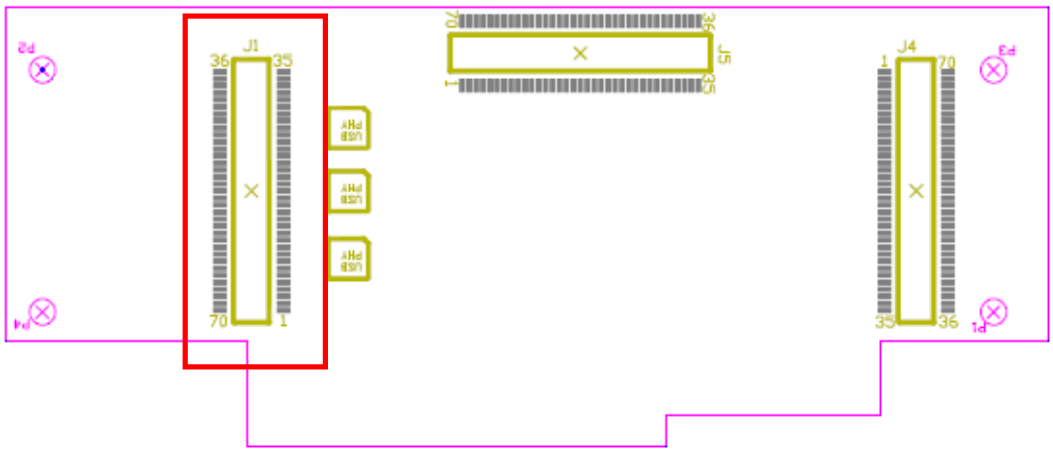


Figure 8.4 – J1 connector hosts

- Digital Display subsystem interface
- Processor McBSP3
- Processor I2C3
- Processor USB-OTG port
- Audio ports
- Analog IN/Out ports
- VGA analog interface (J5 not populated version only)
- 2xUSB 1.1 ports from FPGA (J5 not populated version only)
- Power IN and GND

J1							
Signal group	**Signal**	**Chip**	**pin**		**Chip**	**Signal**	**Signal Group**
	N_MANUAL_RESET		1	70		POWER GND	
LCD INTERFACE DSS	GPIO89_L_DD19/DD01	OMAP	2	69	PMIC	HSORF	Differential single ended headset output
	GPIO88_L_DD18/DD00	OMAP	3	68	PMIC	HSOLF	
	GPIO91_L_DD21/DD03	OMAP	4	67	POWER	POWER VSYSTEM	**Board supply: 3.2V - 4.2V**
	GPIO93_L_DD23/DD05	OMAP	5	66	POWER	POWER VSYSTEM	
	GPIO90_L_DD20/DD02	OMAP	6	65	PMIC	POWERON	Connected to PWRON on PMIC
	GPIO92_L_DD22/D04	OMAP	7	**64**	**OMAP**	**ADCIN7**	**Analog**
	GPIO10_SYSCLK	OMAP	8	**63**	**OMAP**	**GPIO164_RTS3**	**ARM**
	GPIO0_WAKEUP	OMAP	9	**62**	**OMAP**	**GPIO71_DD01**	**CMD for external Pwr-Sw for extrapwr on USB-Otg**
	GPIO185_I2C3_SDA	OMAP	10	61	OMAP	SYSBOOT6/DSS23	LCD INTERFACE DSS
LCD INTERFACE DSS	GPIO80_L_DD10	OMAP	11	60	OMAP	GPIO82_L_DD12	
	GPIO81_L_DD11	OMAP	12	59	PMIC	PMIC_REGEN	
	GPIO184_I2C3_SCL	OMAP	13	**58**	**PMIC**	**ADCIN2**	**Analog Input**
	GPIO186_SYSCLK	OMAP	14	**57**	**PMIC**	**MIC_MAIN_**	**Main microphone letf input**
LCD INTERFACE DSS	SYSBOOT5/DSS22	OMAP	15	56	POWER	POWER GND	
MCBSP3_FSX	GPIO147_GPT8_PWM	OMAP	16	55	OMAP	GPIO145_GPT10_PWM	MCBSP3_DR
LCD INTERFACE DSS	GPIO83_L_DD13	OMAP	17	54	PMIC	USBOTG_VBUS	OMAP USB OTG
MCBSP3_DX	GPIO144_GPT9_PWM	OMAP	18	53	PMIC	ADCIN6	Analog Input
LCD INTERFACE DSS	GPIO84_L_DD14	OMAP	19	52	PMIC	VBACKUP	Backup battery input to PMIC
	GPIO85_L_DD15	OMAP	20	**51**	**PMIC**	**ADCIN5**	**Analog I/O**
MCBSP3_CLK	GPIO146_GPT11_PWM	OMAP	21	**50**	**PMIC**	**AGND**	
OMAP	GPIO179_CTS3	OMAP	22	**49**	**PMIC**	**PWM1**	
LCD INTERFACE DSS	SYSBOOT4/DSS21	OMAP	23	**48**	**PMIC**	**ADCIN3**	
	GPIO87_L_DD17	OMAP	24	47	OMAP	GPIO170_HDQ_1WIRE	1 Wire
	SYSBOOT0/DSS18	OMAP	25	46	PMIC	USBOTG_ID	OMAP USB OTG
FPGA_EXT_UART (1)	**GPIO166_IR_TXD3**	**FPGA**	**26**	45	OMAP	SYSBOOT3/DSS20	LCD INTERFACE DSS
LCD INTERFACE DSS	SYSBOOT1/DSS19	OMAP	27	44	OMAP	GPIO86_L_DD16	
	GPIO79_L_DD09	OMAP	28	43	OMAP	GPIO69_L_BIAS	
	GPIO77_L_DD07	OMAP	29	42	PMIC	PWM0	Analog Output
	GPIO78_L_DD08	OMAP	30	41	PMIC	AUXRF	Auxiliary audio input right
FPGA_EXT_UART (1)	**GPIO165_IR_RXD3**	**FPGA**	**31**	**40**	**PMIC**	**ADCIN4**	**Analog Input**
LCD INTERFACE DSS	GPIO66_L_PCLK	OMAP	32	**39**	**PMIC**	**MIC_SUB_MF**	**Main microphone right input**
	GPIO76_L_DD06	OMAP	33	38	PMIC	AUXLF	Auxiliary audio input left
	GPIO68_L_FCLK	OMAP	34	37	PMIC	USBOTG_DM	OMAP USB OTG
	GPIO67_L_LCLK	OMAP	35	36	PMIC	USBOTG_DP	

(1) 3v3 IO levels

J1							
Signal group	**Signal**	**Chip**	**pin**		**Chip**	**Signal**	**Signal Group**
	N_MANUAL_RESET		1	70		POWER GND	
LCD INTERFACE DSS	GPIO89_L_DD19/DD01	OMAP	2	69	PMIC	HSORF	Differential single ended headset output
	GPIO88_L_DD18/DD00	OMAP	3	68	PMIC	HSOLF	
	GPIO91_L_DD21/DD03	OMAP	4	67	POWER	POWER VSYSTEM	**Board supply: 3.2V - 4.2V**
	GPIO93_L_DD23/DD05	OMAP	5	66	POWER	POWER VSYSTEM	
	GPIO90_L_DD20/DD02	OMAP	6	65	PMIC	POWERON	Connected to PWRON on PMIC
	GPIO92_L_DD22/D04	OMAP	7	**64**	**USBPHY**	**USB_AUX_DM**	**FPGA_USB_HOST_AUX**
	GPIO10_SYSCLK	OMAP	8	**63**	**USBPHY**	**USB_AUX_DP**	**FPGA_USB_HOST_AUX**
	GPIO0_WAKEUP	OMAP	9	**62**	**OMAP**	**GPIO_71_DD01**	**CMD for external Pwr-Sw for extrapwr on USB-Otg**
	GPIO185_I2C3_SDA	OMAP	10	61	OMAP	SYSBOOT6/DSS23	LCD INTERFACE DSS
LCD INTERFACE DSS	GPIO80_L_DD10	OMAP	11	60	OMAP	GPIO82_L_DD12	
	GPIO81_L_DD11	OMAP	12	59	PMIC	PMIC_REGEN	
	GPIO184_I2C3_SCL	OMAP	13	**58**	**USBPHY**	**USB_RADIO_DM**	**USB_RADIO**
	GPIO186_SYSCLK	OMAP	14	**57**	**USBPHY**	**USB_RADIO_DP**	**USB_RADIO**
LCD INTERFACE DSS	SYSBOOT5/DSS22	OMAP	15	56	POWER	POWER GND	
MCBSP3_FSX	GPIO147_GPT8_PWM	OMAP	16	55	OMAP	GPIO145_GPT10_PWM	MCBSP3_DR
LCD INTERFACE DSS	GPIO83_L_DD13	OMAP	17	54	PMIC	USBOTG_VBUS	OMAP USB OTG
MCBSP3_DX	GPIO144_GPT9_PWM	OMAP	18	53	PMIC	ADCIN6	Analog Input
LCD INTERFACE DSS	GPIO84_L_DD14	OMAP	19	52	PMIC	VBACKUP	Backup battery input to PMIC
	GPIO85_L_DD15	OMAP	20	**51**	**VGA**	**RED**	**VGA**
MCBSP3_CLK	GPIO146_GPT11_PWM	OMAP	21	**50**	**VGA**	**VGA_GND**	**VGA**
OMAP	GPIO179_CTS3	OMAP	22	**49**	**VGA**	**GREEN**	**VGA**
LCD INTERFACE DSS	SYSBOOT4/DSS21	OMAP	23	**48**	**VGA**	**BLUE**	**VGA**
	GPIO87_L_DD17	OMAP	24	47	OMAP	GPIO170_HDQ_1WIRE	1 Wire
	SYSBOOT0/DSS18	OMAP	25	46	PMIC	USBOTG_ID	OMAP USB OTG
FPGA_EXT_UART (1)	**GPIO166_IR_TXD3**	**FPGA**	**26**	45	OMAP	SYSBOOT3/DSS20	LCD INTERFACE DSS
LCD INTERFACE DSS	SYSBOOT1/DSS19	OMAP	27	44	OMAP	GPIO86_L_DD16	
	GPIO79_L_DD09	OMAP	28	43	OMAP	GPIO69_L_BIAS	
	GPIO77_L_DD07	OMAP	29	42	PMIC	PWM0	Analog Output
	GPIO78_L_DD08	OMAP	30	41	PMIC	AUXRF	Auxiliary audio input right
FPGA_EXT_UART (1)	**GPIO165_IR_RXD3**	**FPGA**	**31**	**40**	**VGA**	**H_SYNC**	**VGA**
LCD INTERFACE DSS	GPIO66_L_PCLK	OMAP	32	**39**	**VGA**	**V_SYNC**	**VGA**
	GPIO76_L_DD06	OMAP	33	38	PMIC	AUXLF	Auxiliary audio input left
	GPIO68_L_FCLK	OMAP	34	37	PMIC	USBOTG_DM	OMAP USB OTG
	GPIO67_L_LCLK	OMAP	35	36	PMIC	USBOTG_DP	

(1) 3v3 IO levels

Figure 8.5 – J1 pinout (J5 not populated version)

J4 expansion connector

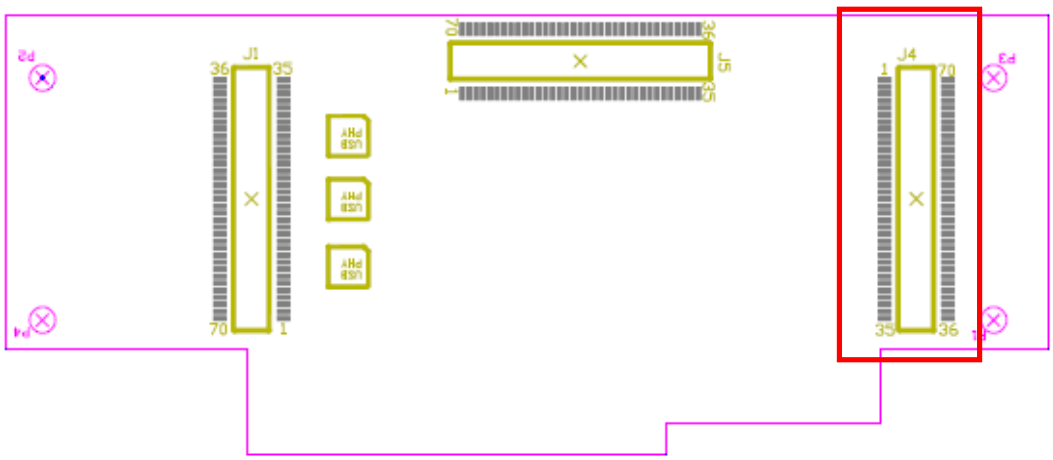


Figure 8.6 – J4 connector hosts:

- Processor MMC3
- Processor SPI1
- Processor USB-HOST port
- Processor Parallel BUS
- Power IN and GND

J4							
Signal group	**Signal**	**Chip**	**pin**		**Chip**	**Signal**	**Signal Group**
Board supply: 3.2V - 4.2V	POWER VSYSTEM	POWER	1	70	**OMAP**	**GPMC_CLK**	
	POWER VSYSTEM	POWER	2	69	**OMAP**	**GPMC_nBE1**	
	POWER GND	POWER	3	68	**OMAP**	**GPMC_WAIT0**	
Parallel BUS	**GPMC_NCS5**	**OMAP**	4	67	**OMAP**	**GPMC_NCS6**	
	GPMC_NCS4	**OMAP**	5	66	**OMAP**	**GPMC_NCS0**	
	GPMC_nWE	**OMAP**	6	65	**OMAP**	**GPMC_nBE0**	
	GPMC_NADV_ALE	**OMAP**	7	64	**OMAP**	**GPMC_NCS1**	
	GPMC_nOE	**OMAP**	8	63	**OMAP**	**GPMC_nWP**	
	GPMC_WAIT3/ UART4_TX	**OMAP**	9	62	**OMAP**	**GPMC_A9**	
	GPMC_WAIT2/ UART4_RX	**OMAP**	10	61	**OMAP**	**GPMC_A4**	
	GPMC_A2	**OMAP**	11	60	**OMAP**	**GPMC_A10**	**Parallel BUS**
	GPMC_A8	**OMAP**	12	59	**OMAP**	**GPMC_A3**	
	GPMC_A5	**OMAP**	13	58	**OMAP**	**GPMC_A1**	
	GPMC_A7	**OMAP**	14	57	**OMAP**	**GPMC_A6**	
	GPMC_D2	**OMAP**	15	56	**OMAP**	**GPMC_D0**	
	GPMC_D10	**OMAP**	16	55	**OMAP**	**GPMC_D9**	
	GPMC_D3	**OMAP**	17	54	**OMAP**	**GPMC_D8**	
	GPMC_D11	**OMAP**	18	53	**OMAP**	**GPMC_D1**	
	GPMC_D4	**OMAP**	19	52	**OMAP**	**GPMC_D13**	
	GPMC_D12	**OMAP**	20	51	**OMAP**	**GPMC_D6**	
	GPMC_D5	**OMAP**	21	50	**OMAP**	**GPMC_D14**	
	GPMC_D15	**OMAP**	22	49	**OMAP**	**GPMC_D7**	
MMC3 INTERFACE	GPIO13_MMC3_CMD	OMAP	23	48	**FPGA**	**GPMC_RXD1**	**FPGA_RADIO_UART (1)**
FPGA_RADIO_UART (1)	**GPMC_TXD1**	**FPGA**	24	47	OMAP	PMIC_GPIO15_MMC3_ WP	MMC3 INTERFACE
SPI1 INTERFACE/ETH0_IRQ	GPIO176_SPI1_CS2	OMAP	25	46	OMAP	PMIC_GPIO02_MMC3_ CD	
MMC3 INTERFACE	GPIO18_MMC3_D0	OMAP	26	45	OMAP	GPIO173_SPI1_MISO	SPI1 INTERFACE
SPI1 INTERFACE	GPIO174_SPI1_CS0	OMAP	27	44	OMAP	GPIO172_SPI1_MOSI	
OMAP USB HOST (HS): CMDout for +5V external USB switch	**GPIO70_DD00**	**OMAP**	28	43	OMAP	GPIO171_SPI1_CLK	
MMC3 INTERFACE	GPIO14_MMC3_D4	OMAP	29	42	OMAP	GPIO175_SPI1_CS1	
	GPIO21_MMC3_D7	OMAP	30	41	OMAP	GPIO114_SPI1_NIRQ	
	GPIO17_MMC3_D3	OMAP	31	40	OMAP	GPIO12_MMC3_CLK	MMC3 INTERFACE
OMAP USB HOST (HS)	USBH_VBUS_IN	USB-PHY	32	39	OMAP	GPIO20_MMC3_D2	
	POWER GND	POWER	33	38	OMAP	GPIO23_MMC3_D5	
OMAP USB HOST (HS)	USBH_DP	USB-PHY	34	37	OMAP	GPIO22_MMC3_D6	
	USBH_DM	USB-PHY	35	36	OMAP	GPIO19_MMC3_D1	

(1) 3v3 IO levels

Figure 8.7 – J4 pinout (J5 populated and not populated version)

J5 expansion connector

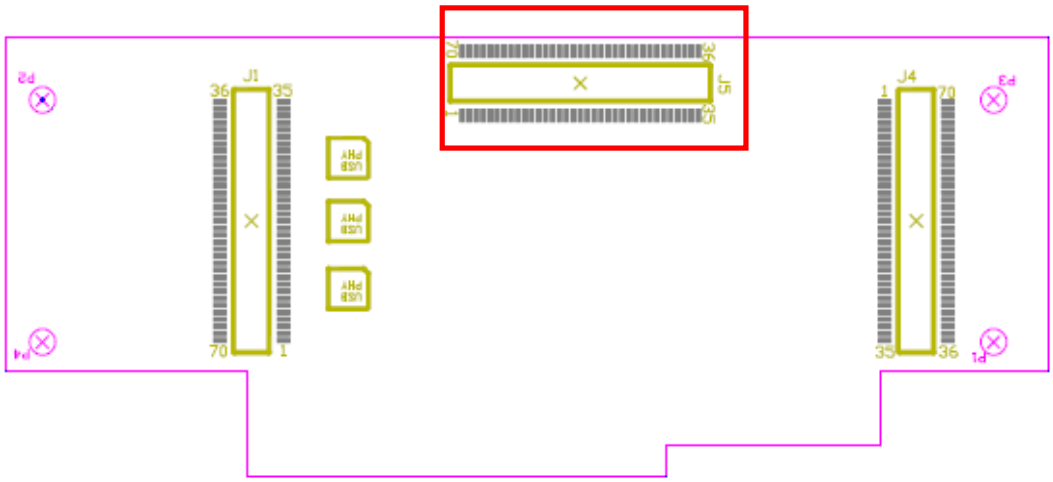


Figure 8.8 – J5 connector hosts

- Processor TVout (secondary Frame Video analog channel)
- VGA analog interface
- 2xUSB 1.1 ports from FPGA
- Processor camera interface
- Processor I2C2
- Processor I2C3
- FPGA user configurable pins
- Power IN and GND

J5							
Signal group	**Signal**	**Chip**	**pin**	**pin**	**Chip**	**Signal**	**Signal Group**
TV out	TV_OUT2R	OMAP	1	**70**	**USB_ PHY**	**FPGA_USB_AUX_DP**	**FPGA HOST/DEVICE**
	TV_OUT1R	OMAP	2	**69**	**USB_ PHY**	**FPGA_USB_AUX_DM**	
	POWER GND	POWER	3	**68**	**FPGA**	**FPGA_USB_AUX_VBUS**	
VGA	**RED**	**R2R**	**4**	**67**	**FPGA**	**FPGA_USB_AUX_CMD**	**USB AUX HOST (FS): CMDout for +5V external USB switch (3v3 level)**
	VGA_GND	**POWER**	**5**	**66**	**USB_ PHY**	**FPGA_USB_RADIO_DP**	**FPGA HOST**
	GREEN	**R2R**	**6**	**65**	**USB_ PHY**	**FPGA_USB_RADIO_DM**	
	VGA_GND	**POWER**	**7**	64	OMAP+ FPGA	GPIO168_I2C2_SCL/FPGA_SPARE_1V8_IO26	I2C2 paralled to FPGA
	BLUE	**R2R**	**8**	63	OMAP+ FPGA	GPIO183_I2C2_SCL/FPGA_SPARE_1V8_IO25	
PMIC VOLTAGE	**VDDS_1.8**	**PMIC**	**9**	62	FPGA	FPGA_SPARE_1V8_IO20	FPGA configurable PINS 1.8Vcc
VGA	**VSYNC/KPD_C0**	**R2R**	**10**	61	FPGA	FPGA_SPARE_1V8_IO19	
	HSYNC/KPD_C1	**R2R**	**11**	60	FPGA	FPGA_SPARE_1V8_IO18	
KEYBOARD	**KPD_C2**	**PMIC**	**12**	59	FPGA	FPGA_SPARE_1V8_IO17	
Camera Interface	GPIO94_CAM_HS	OMAP	13	58	FPGA	FPGA_SPARE_1V8_IO16	
	GPIO95_CAM_VS	OMAP	14	57	FPGA	FPGA_SPARE_1V8_IO15	
	GPIO96_CAM_XclkA	OMAP	15	56	FPGA	FPGA_SPARE_1V8_IO14	
	GPIO97_CAM_PCLK	OMAP	16	55	FPGA	FPGA_SPARE_1V8_IO13	
	GPIO98_CAM_FLD	OMAP	17	54	FPGA	FPGA_SPARE_1V8_IO12	
	GPIO99_CAM_D0	OMAP	18	53	FPGA	FPGA_SPARE_1V8_IO11	
	GPIO100_CAM_D1	OMAP	19	52	FPGA	FPGA_SPARE_1V8_IO10	
	GPIO101_CAM_D2	OMAP	20	51	FPGA	FPGA_SPARE_1V8_IO9	
	GPIO102_CAM_D3	OMAP	21	50	FPGA	FPGA_SPARE_1V8_IO8	
	GPIO103_CIF_DD04	OMAP	22	49	FPGA	FPGA_SPARE_1V8_IO7	
	GPIO104_CIF_DD05	OMAP	23	48	FPGA	FPGA_SPARE_1V8_IO6	
	GPIO105_CAM_D6	OMAP	24	47	FPGA	FPGA_SPARE_1V8_IO5	
	GPIO106_CIF_DD07	OMAP	25	46	FPGA	FPGA_SPARE_1V8_IO4	
	GPIO107_CIF_DD08	OMAP	26	45	FPGA	FPGA_SPARE_1V8_IO3	
	CPIO108_CIF_DD09	OMAP	27	44	FPGA	FPGA_SPARE_1V8_IO2	
	GPIO109_CAM_D10	OMAP	28	43	FPGA	FPGA_SPARE_1V8_IO1	
	GPIO110_CAM_D11	OMAP	29	42	FPGA	FPGA_SPARE_3V3_IO7	
	GPIO111_CAM_XCLKB	OMAP	30	41	FPGA	FPGA_SPARE_3V3_IO6	
	GPIO167_CAM_WEN	OMAP	31	40	FPGA	FPGA_SPARE_3V3_IO5	
	GPIO126_CAM_STROBE	OMAP	32	39	FPGA	FPGA_SPARE_3V3_IO4	
	GPIO63_CAM_IRQ	OMAP	33	38	FPGA	FPGA_SPARE_3V3_IO3	FPGA configurable PINS 3v3Vcc
	GPIO184_I2C3_SCL	OMAP	34	37	FPGA	FPGA_SPARE_3V3_IO2	
	GPIO185_I2C3_SDA	OMAP	35	36	FPGA	FPGA_SPARE_3V3_IO1	

Figure 8.9 – J5 pinout

8.2 J7 JTAG connector

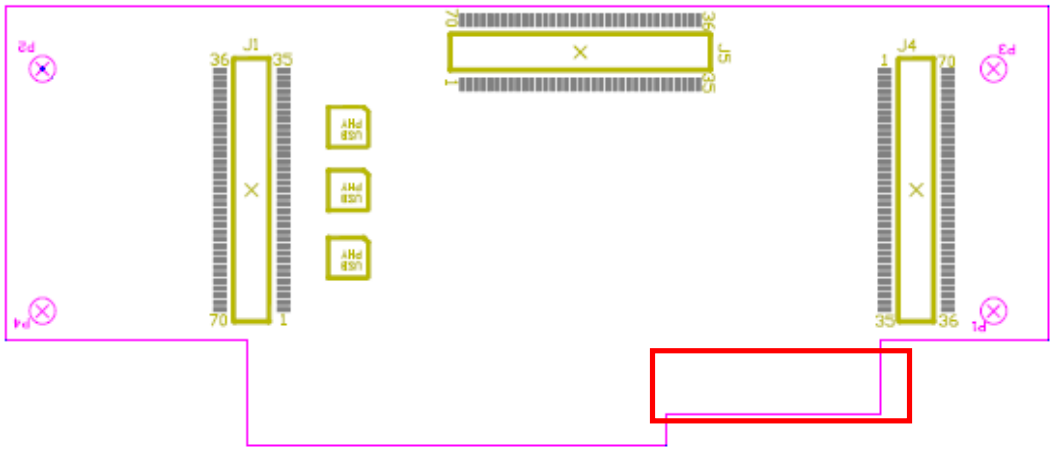


Figure 8.10 – J7 connector hosts

- Processor JTAG/EMU interface
- FPGA JTAG interface
- Power IN and GND

J7			
Signal	**pin**	**IC-signal**	**Signal group**
OMAP_JTAG_TMS	**1**	**OMAP**	**OMAP JTAG or BT interface**
OMAP_JTAG_TDI	**2**	**OMAP**	
OMAP_JTAG_TD	**3**	**OMAP**	
OMAP_JTAG_TCK	**4**	**OMAP**	
JTAG_EMU1	**5**	**OMAP**	
JTAG_EMU0	**6**	**OMAP**	
JTAG_nTRST	**7**	**OMAP**	
JTAG_RTCK	**8**	**OMAP**	
POWER GND	9	POWER	GROUND
	10	POWER	
FPGA_JTAG_TMS	**11**	**TPS65950**	**FPGA_JTAG**
FPGA_JTAG_TDI	**12**	**TPS65950**	
FPGA_JTAG_TD	**13**	**TPS65950**	
FPGA_JTAG_TCK	**14**	**TPS65950**	
Board supply: 3.2V - 4.2V	15	POWER	GROUND
	16	POWER	

Figure 8.11 – J7 pinout

For testing and developing SW on the OMBRAv2-pShield Board a Carrier Test board is available, giving smart access to the interface available.

A block diagram of the carrier board is showed below.

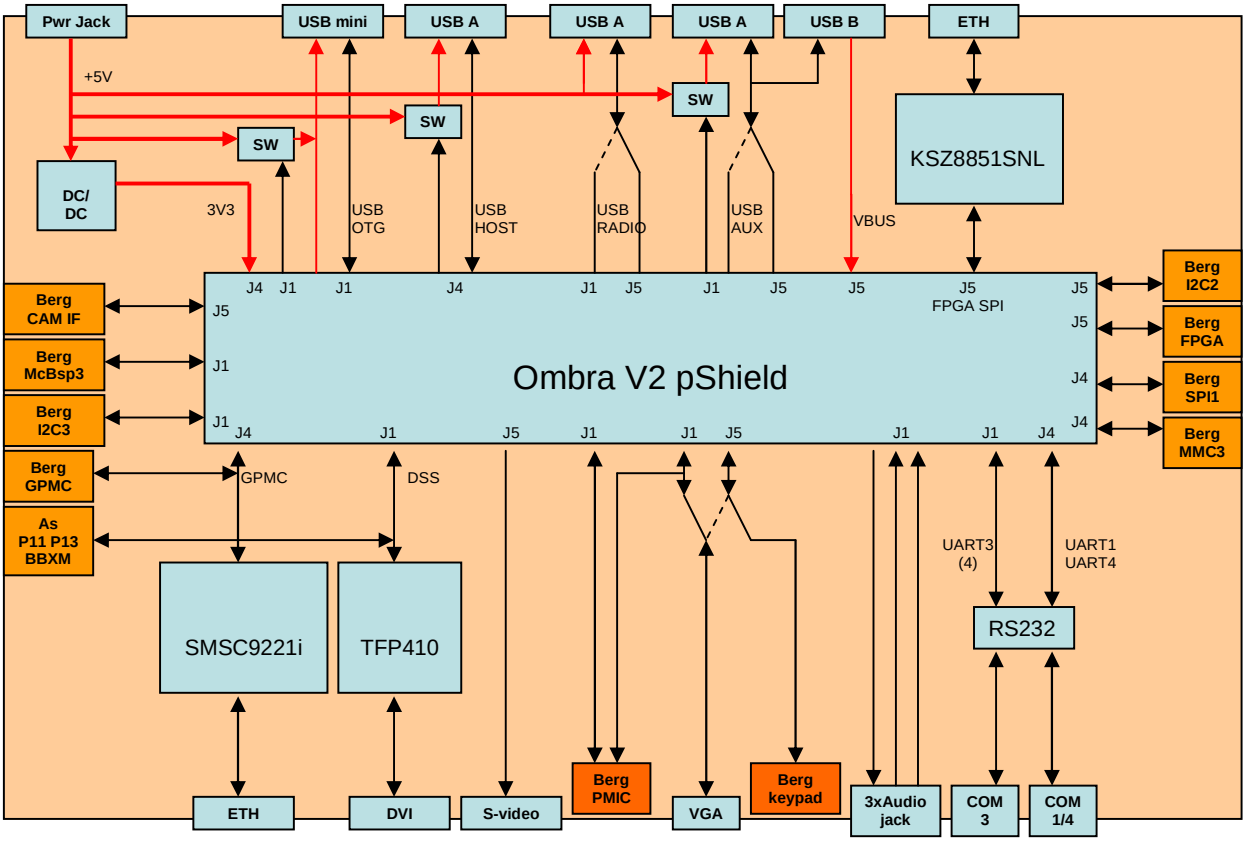
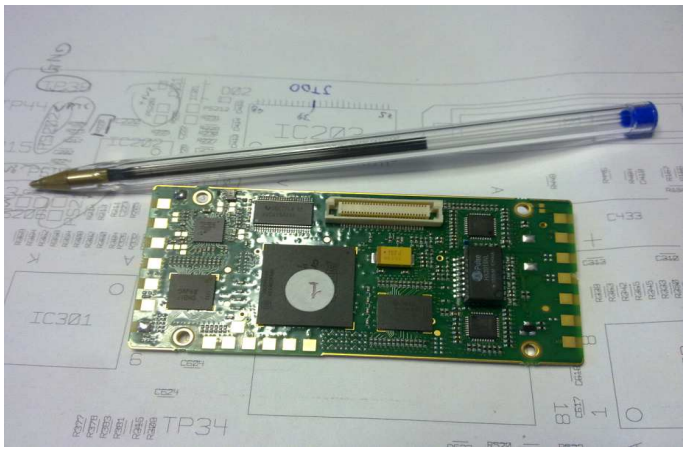


Figure 8.12 – Test carrier board Block Diagram



Carrier Board (40x80mm)

PCB OMAP (18x68mm)
Computational Power 5X
WCP (1K pcs) =~ 100 Euro

PCB Standard with PXA270
110x130mm WCP =~ 350Euro

Figure 8.13 – Comparison with standard pcb

9 Terminal Characteristics

Proposed radio terminal will have the following characteristics:

- type	handheld
- sdr capability	compliant to SCA
- RF band	30 ÷ 500 MHz
- Tx power	5 W
- bandwidth	up to 2 MHz
- power supply	battery operated
- user interface	data (USB, Ethernet) and analog voice
- MMI interface	graphical color LCD display keyboard
- security	encryption, password protection, access authentication
- auxiliary functions	embedded GPS receiver headset extension

Due to the SDR nature of the terminal, several parameters like modulation format, transmission mode, channel bandwidth, encryption algorithm, MAC and routing protocol are fully programmable under the control of the waveform SW.

Main parameters of the broadband waveform that will be used for the scope of this work are given for reference:

- frequency range	225 ÷ 512 MHz
- transmission mode	TDD
- access mode	TDMA
- modulation	QPSK
- channel width	1.3 MHz
- net throughput	500 kb/s
- max hops	5
- active subscribers	32
- call capabilities	unicast, multicast, broadcast
- groups	up to 9 voice groups, up to 9 data VLANs
- routing	static IP V4

10 References

[1] L. Bai, D. Chou, D. Yen, and B. Lin, “Mobile commerce: its market analyses,” International Journal of Mobile Communications, vol. 3, no. 1, pp. 66-81, 2005.

[2] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” IEEE J. Sel. Areas Comm., vol. 23, no. 2, pp. 201-220, Feb. 2005.

[3] B. A. Fette, Cognitive Radio Technology. Oxford: Newnes, 2006.

[4] L. Bixio, A. F. Cattoni, C. S. Regazzoni, and P. K. Varshney, Autonomic Computing and Networking. Springer, New York, 2009, ch. Embodied Cognition-Based Distributed Spectrum Sensing for Autonomic Wireless Systems.

[5] R. Doyle, E. Dupuis, M. Oda, J.-C. Piedbeouf, and G. Visentin, “Progress on AI, Robotics, and Automation in Space: A Report from i-SAIRAS 08,” IEEE Intelligent Systems, vol. 24, no. 1, pp. 78-83, 2009.

[6] DARPA XG WG, “The XG Architectural Framework v1.0,” DARPA, Tech. Rep., 2003.

[7] P. Kolodzy, “Next Generation communications: Kickoff meeting,” in Proc. DARPA, October 2001.

[8] M. Khoshkholgh, K. Navaie, and H. Yanikomeroglu, “Access strategies for spectrum sharing in fading environment: Overlay, underlay, and mixed,” IEEE Transactions on Mobile Computing, vol. 9, no. 12, pp. 1780-1793, 2010.

[9] L. Bixio, G. Oliveri, M. Ottonello, M. Raffetto, and C. Regazzoni, “Cognitive radios with multiple antennas exploiting spatial opportunities,” IEEE Trans. Signal Process., vol. 58, no. 8, pp. 4453-4459, Aug. 2010.

[10] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 116-130, First Quarter 2009.

[11] R. Zhang and Y.-C. Liang, “Exploiting Multi-Antennas for Opportunistic Spectrum Sharing in Cognitive Radio Networks,” IEEE J. Sel. Topics. Signal Process, vol. 2, no. 1, pp. 88-102, Feb. 2008.

[12] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey,” Computer Networks, vol. 50, pp. 2127-2159, May 2006.

[13] H. Urkowitz, “Energy Detection of unknown deterministic signals,” Proceedings of IEEE, vol. 55, no. 4, pp. 523-531, April 1967.

[14] W. A. Gardner, “Signal Interception: A Unifying Theoretical Framework for Feature Detection,” IEEE Transactions on Communications, vol. 36, no. 8, pp. 897-906, August 1988.

[15] E. Azzouz and A. Nandi, Automatic Modulation Recognition of Communication Signals. Kluwer Academic Publishers Norwell, MA, USA, 1996.

[16] C. K. Chen and W. A. Gardner, “Signal-Selective Time-Difference-of-Arrival Estimation for Passive Location of Man-Made Signal Sources in Highly Corruptive Environments, Part II: Algorithms and Performance,” IEEE Transactions on Signal Processing, vol. 40, no. 5, pp. 1185-1197, May 1992.

[17] D. Cabric, S. M. Mishra, and R. W. Brodersen, “Implementation issues in spectrum sensing for cognitive radios,” in Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, Nov. 2004, pp. 772-776.

[18] A. Ghasemi and E. S. Sousa, “Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs,” IEEE Communications Magazine, vol. 46, no. 4, pp. 32-39, Apr. 2008.

[19] S. Geirhofer, L. Tong, and B. M. Sadler, “Dynamic spectrum access in the time domain: modeling and exploiting white space,” IEEE Comm. Mag., vol. 45, no. 5, pp. 66-72, May 2007.

[20] L. Bixio, M. Ottonello, M. Raffetto, and C. S. Regazzoni, “Performance evaluation of a multiple antenna system for spectrum sensing,” in IEEE International Symposium on Antennas & Propagation, North Charleston, South Carolina, Jun. 1-5 2009.

[21] R. Hachemani, J. Palicot, and C. Moy, “A new standard recognition sensor for cognitive terminal,” in Proceeding of the European Signal Processing Conference, 2007.

[22] K. Ahmad, U. Meier, and H. Kwasnicka, “Fuzzy logic based signal classification with cognitive radios for standard wireless technologies,” in Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks & Communications (CROWNCOM), Cannes, France, Jun. 2010, pp. 1-5.

[23] S. Qian and D. Chen, “Joint time-frequency analysis,” IEEE Signal Processing Magazine, vol. 16, no. 2, pp. 52-67, Mar. 1999.

[24] M. Oner and F. Jondral, “On the extraction of the channel allocation information in spectrum pooling systems,” IEEE J. Sel. Areas Comm., vol. 25, no. 3, pp. 558-565, April 2007.

[25] P. Sutton, K. Nolan, and L. Doyle, “Cyclostationary Signatures in Practical Cognitive Radio Applications,” IEEE J. Sel. Areas Comm., vol. 26, no. 1, pp. 13-24, January 2008.

[26] A. Fehske, J. Gaeddert, and J. Reed, “A new approach to signal classification using spectral correlation and neural networks,” in First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, MD, USA, Nov. 2005, pp. 144-150.

[27] K. Kim, I. Akbar, K. Bae, J. sun Urn, C. Spooner, and J. Reed, “Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio,” in Second IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Dublin, Ireland, Apr. 2007, pp. 212-215.

[28] M. M. Kokar, D. Brady, K. Baclaski, “Roles of Ontologies in Cognitive Radios,” in B. Fette, Cognitive Radio Technologies, ELSEVIER, USA.

[29] A. Jain, R. Duin, and J. Mao, “Statistical pattern recognition: a review,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 4-37, Jan. 2000.

[30] R. Lippmann, “Pattern classification using neural networks,” IEEE Communications Magazine, vol. 27, no. 11, pp. 47-50,59-64, Nov. 1989.

[31] B. Ramkumar, “Automatic modulation classification for cognitive radios using cyclic feature detection,” IEEE Circuits and Systems Magazine, vol. 9, no. 2, pp. 27-45, Second Quarter 2009.

[32] L. Bixio, M. Ottonello, M. Raffetto, and C. S. Regazzoni, “OFDM recognition based on cyclostationary analysis in an open spectrum scenario,” in IEEE 69th Vehicular Technology Conference 2009, Barcelona, Spain, Apr. 26-29 2009.

[33] V. Kecman, Learning and Soft Computing: Support Vector Machines, Neural Networks, and Fuzzy Logic Models. The MIT Press, 2001.

[34] S. Gunn, “Support vector machine for classification and regression,” Univ. Southampton, Southampton, U.K., Tech. Rep., May 1998. [Online]. Available: http://www.isis.ecs.soton.ac.uk/resource/svminfo/.

[35] C.-C. Chang and C.-J. Lin, LIBSVM: a library for support vector machines, 2001, software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[36] C. wei Hsu, C. chung Chang, and C. jen Lin, “A practical guide to support vector classification,” Department Of Computer Science National Taiwan University, Taipei 106, Taiwan, Tech. Rep., May 2008. [Online]. Available: http://www.csie.ntu.edu.tw/~cjlin/.

[37] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, “Toward secure distributed spectrum sensing in cognitive radio networks,” IEEE Communications Magazine, vol. 46, no. 4, pp. 50-55, Apr. 2008.

[38] C. Bishop, Pattern Recognition and Machine Learning. Springer, 2006.

[39] A. Goldsmith, Wireless Communications, 1st ed. Cambridge, UK: Cambridge University Press, 2005.

[40] T. S. Rappaport, Wireless Communications: Principles and Practice, 2nd ed. Prentice Hall, Jan. 2002.

[41] W. C. Y. Lee, Mobile Communications Engineering: Theory and Applications, 2nd ed. McGraw-Hill Professional, Oct. 1997.

[42] M. Gandetto, C. S. Regazzoni, “Spectrum sensing: a distributed approach for cognitive terminals,” IEEE J. Sel. Areas Comm., vol. 25, no. 3, pp. 546-557, Apr. 2007.

[43] P. K. Varshney, Distributed Detection and Data Fusion, 1st ed. Springer-Verlag, 1996.

[44] Arslan Hüseyin, SŞhin, Mustafa, “UWB Cognitive Radio,” in Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems, ed. Arslan Hüseyin, Springer Netherlands, pp. 355-381, 2007, URL: http://www.springerlink.com/content/v512609354086622/fulltext.pdf

[45] Arslan Hüseyin, Mahmoud Hisham, Yücek, Tevfik, “OFDM for Cognitive Radio: Merits and Challenges,” in Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems, ed. Arslan Hüseyin, Springer Netherlands, pp. 325-353, 2007, URL: http://www.springerlink.com/content/x38276g104261127/fulltext.pdf

[46] L. Lu et al., “Technology Proposal Clarifications for IEEE 802.22 WRAN Systems,” IEEE 802.22 WG on WRANs, Mar. 2006.

[47] R. Chen, J.-M. Park, J.H. Reed; , “Defense against Primary User Emulation Attacks in Cognitive Radio Networks,” IEEE Journal on Selected Areas in Communications, vol.26, no.1, pp. 25-37, Jan. 2008.

[48] D. Pauluzzi and N. Beaulieu, “A comparison of SNR estimation techniques for the AWGN channel,” IEEE Transactions on Communications, vol. 48, no. 10, pp. 1681–1691, Oct. 2000.

[49] A. Wiesel, J. Goldberg, and H. Messer-Yaron, “SNR estimation in time-varying fading channels,” IEEE Transactions on Communications, vol. 54, no. 5, pp. 841–848, May 2006.

[50] R. Chen and J.-M. Park, “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks,” in Proceedings of the IEEE Workshop on Networking Technologies for Software Defined Radio Networks, Sept. 2006, pp. 110–19.

[51] Y. Zhao *et al.*, “Overhead Analysis for Radio Environment Map-Enabled Cognitive Radio Networks” in Proceedings of the IEEE Workshop on Networking Technologies for Software Defined Radio Networks, Sept. 2006, pp. 18–25.

[52] J.L. Burbank, “Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security,” 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008, pp. 1-7, 15-17 May 2008.

[53] A. Pandharipande *et al.*, “IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22,” IEEE 802.22 WG on WRANs, Nov. 2005.

[54] L. Bixio, M. Ottonello, M. Raffetto, C.S. Regazzoni, C. Armani, “A comparison among cooperative spectrum sensing approaches for cognitive radios,” *2nd International Workshop on Cognitive Information Processing (CIP), 2010*, pp. 168-173, 14-16 June 2010.

[55] J. Hillenbrand, T. A. Weiss, and F. K. Jondral, “Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems,” *IEEE Commun. Lett.*, vol. 9, no. 4, Apr. 2005, pp. 349-51.