SPD-driven Smart Transmission Layer based on a Software Defined Radio Test Bed Architecture

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

Keywords: Cognitive Radio, Software Defined Radio, Smart Transmission Layer, Security, Privacy, Dependability, nSHIELD, Test Bed, SDR, CR, Jamming, Energy Detector Spectrum Sensing.

Abstract: Cognitive Radio as a technological breakthrough and enabler for concepts such as Opportunistic Spectrum Access and Dynamic Spectrum Access has so far received significant attention from the research community from a theoretical standpoint. In this work, we build upon the theoretical foundation and present an implementation of a Software Defined Radio/Cognitive Radio platform, with the feature under particular interest being the so-called Smart Transmission Layer. Smart Transmission Layer is a feature developed within the currently ongoing nSHIELD project, whose goal is establishing new paradigms for Security, Privacy and Dependability (SPD) of the future embedded systems. The role of the SPD-driven Smart Transmission Layer is providing reliable and efficient communications in critical channel conditions by using adaptive and flexible algorithms for dynamically configuring and adapting various transmission-related parameters. The implementation was done on the test bed consisting of two Secure Wideband Multi-role - Single-Channel Handheld Radios (SWAVE HH) coupled with the powerful proprietary multi-processor embedded platforms, and the corresponding auxiliaries. Several case studies were performed, namely: remote control of the radios, analysis of the installed waveforms, interference detection, and spectrum sensing using a quasi-real-time energy detector. A roadmap towards the future implementation aspects using the test bed was set.

1 INTRODUCTION

With the continuous market penetration of many spectrum-demanding radio-based services, such as video broadcasting, finding ways to increase the spectrum usage efficiency has become a necessity. Cognitive Radio (CR) is a technological breakthrough that is expected to be an enabler for these improvements by utilizing concepts such as Opportunistic Spectrum Access (OSA) and Dynamic Spectrum Access (DSA), making it a current hot topic within the radio communication research community. Cognitive radio can be described as an intelligent and dynamically reconfigurable radio that can adaptively regulate its internal parameters in response to the changes in the surrounding environment. Namely, its parameters can be reconfigured in order to accommodate the current needs of either the network operator, spectrum lessor, or the end-user.

Cognitive Radio (Mitola and Maguire, 1999) is commonly defined as an upgraded and enhanced Software Defined Radio (SDR). Typically, full Cognitive Radios will have learning mechanisms based on some of the existing machine learning techniques, and in addition may potentially be equipped with smart antennas, geolocation capabilities, biometrical identification and so on (Fette, 2006).

However, the newly-introduced cognitive capabilities are precisely what make Cognitive Radios susceptible to a whole new set of security issues and possible breaches (Dabcevic et al., 2013). In addition, SDR-based CRs inherit the vulnerabilities characteristic to Software Defined Radios, as well as the security issues stemming out from their wireless nature (Fragkiadakis et al., 2013). Addressing all of the aforementioned is, therefore, paramount for ensuring the secure, fault-tolerant operation of future Cognitive Radio Networks.

Addressing security, privacy and dependability issues, and providing safe and robust communication in Software Defined Radio and Cognitive Radio Networks is role of the SPD-driven Smart Transmission Layer - one of the features of the nSHIELD (new Systems arcHItecturE for multi-Layer Dependable solutions) framework. This paper gives an overview of the SDR test bed architecture that will be used for devel-

Dabcevic K., Marcenaro L. and Regazzoni C..
SPD-driven Smart Transmission Layer based on a Software Defined Radio Test Bed Architecture.
DOI: 10.5220/0004876302190230
In *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems* (MeSeCCS-2014), pages 219-230
ISBN: 978-989-758-000-0
Copyright © 2014 SCITEPRESS (Science and Technology Publications, Lda.)

opment and experimentation of various Smart Transmission Layer features, providing proof-of-concept in terms of demonstrating several important functionalities that will aid future research.

Wireless communication is fundamentally susceptible to variation and upset due to the nature of the transmission medium, nodes mobility, noise, and interference. Because of that, it was decided to assemble a simulated RF bench, which exhibits several clear-cut advantages compared to over-the-air transmission, namely:

- possibility of setting accurate and stable RF levels,
- test instruments and generators can be connected to one or more branches,
- possibility of mimicking complex dynamic behaviors of the transmission channel,
- replicability of the tests without the typical uncertainties of over-the-air transmission.

The remainder of this work is structured as follows: related work on Software Defined Radio and Cognitive Radio platforms and test beds is given in section 2. Section 3 presents the ideas and premises driving the nSHIELD project, as well as the architectural overview of the nSHIELD-compliant devices and systems. Implementation details of the proposed SDR/CR test bed architecture are given in section 4, whereas exercised functionalities that have reached demonstrable level are described in section 5, along with the experiment results. Conclusions and the roadmap are presented in section 6.

2 EXISTING COGNITIVE RADIO TEST BEDS AND PLATFORMS

Software Defined Radios and Cognitive Radios were given significant attention from the research community over the last years. However, most of the contributions have focused on theoretical modeling and analysis. As useful as the simulation environment is for the algorithm research and development, simulators of wireless systems necessarily introduce many abstractions, often leading to losing track of important real-life constraints and obstacles. As such, demonstrating effectiveness of wireless systems' cognitive features on a simulation basis only is not sufficient. Instead, these features need to be executed and evaluated on real-life test beds.

Researchers at the Berkeley Wireless Research Center have developed an experimental cognitive radio platform based on the Berkeley Emulation Engine (BEE2), and reconfigurable 2.4 GHz RF front ends, using fiber links for inter-communication. BEE2 engine consisted of five Xilinx Virtex-2 Field Programmable Gate Arrays (FPGAs), and supported connection of up to 18 individual RF front-ends, making the Multiple Input Multiple Output (MIMO) experimentation possible. The RF front-ends supported up to 25 MHz bandwidth in a 85 MHz frequency range. All signal processing was being done directly on the platform. The software architecture was based on Matlab Simulink, coupled with the Xilinx System Generator library enhanced by a set of blocks in order to support interfaces with Analog-to-Digital Converters and Double data rate (DDR) memory. The majority of the focus of the research was placed upon the spectrum sensing implementations, showing the practical performance and constraints of energy detectors (Cabric et al., 2006) and cyclostationary feature detectors (Tkachenko et al., 2006) in imperfect channel conditions.

Kansas University Agile Radio (KUAR) (Minden et al., 2007) was a low-cost experimental SDR platform based on an embedded 1.4 GHz General Purpose Processor (GPP), Xilinx Virtex-2 FPGA, and a RF front-end with 30 MHz bandwidth. The RF front-end was designed to operate in the 5-6 GHz frequency band. The majority of the signal processing was delegated to the FPGA, which is targeted using the software libraries running Linux OS. KUAR's software architecture consisted of a set of Application Programming Interfaces (APIs), comprising the KUAR Control Library. The research topics up to date included implementation of agile transmission techniques; distributed radio spectrum survey, and channel sounding techniques.

Maynooth Adaptable Radio System (MARS) (Farrell et al., 2009) was another experimental SDR/CR platform, consisting of an RF front end interconnected with a personal computer, where all the signal processing burden was placed on the PC's GPP. The platform operated in the 1.75-2.45 GHz range, with the direct conversion architecture implemented both at the transmitting and the receiving side. The proprietary software architecture, called IRiS, was highly reconfigurable, and was compatible with both Windows and Linux. A set of use-cases, such as spectrum sensing; image and video transmission, and interoperability with other SDR platforms, was studied and implemented using the platform.

3 nSHIELD - APPLICATION OF SECURITY, PRIVACY AND DEPENDABILITY IN THE CONTEXT OF EMBEDDED SYSTEMS

Ever-increasing complexity and scope of capabilities of modern communication devices and systems inherently bring a set of new security and dependability issues. In the domain of embedded systems, especially those consisting of constrained low-end devices, implementation of appropriate security measures is often not adequately addressed.

Providing a complete, unified framework for Security, Privacy and Dependability (SPD) for a variety of embedded devices and systems is the goal of the currently-ongoing nSHIELD project (nSHIELD Consortium, 2012). nSHIELD framework envisions a system architecture (see Figure 1) that consists of four functional layers: three horizontal ones - Node, Network and Middleware, all comprehended by the single vertical layer called Overlay. The SPD functionalities are exercised at each of the horizontal layers, with the Overlay layer having a logical operational control, i.e. being in charge of decision-making with respect to which of the SPD functionalities are to be activated/deactivated at a particular time instance in order to reach a desired SPD level. Desired SPD level can either be imposed manually by the operator or, in case of intelligent automated systems, by the corresponding cognitive entity.

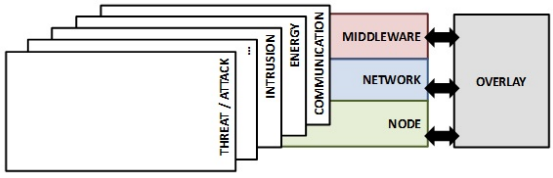

Figure 1: nSHIELD system architecture.

The Node layer encompasses physical elements that constitute the nSHIELD network, and can be divided into three basic types of embedded devices, distinguishable mainly by their computational capabilities and power restrictions:

- Nano nodes – constrained battery-powered nodes with low computational capabilities and low reconfigurability potentials. They typically require a set of lightweight security protocols, and are capable of running light operating system, i.e. EasyOS, ContikiOS or Arduino. Nano nodes can further be subdivided into nSHIELD-enabled nano nodes and nSHIELD-compliant nano nodes, where the first ones are capable of deploying one or more of the SPD functionalities, whereas the latter ones don't have the SPD functionalities embodied, but are able to communicate and interoperate with the nSHIELD-enabled nodes. Examples of currently available commercial embedded platforms that correspond to the definition of Nano nodes are e.g. Zolertia Z1 (Zolertia, 2013), Arduino Uno (Arduino, 2013) and Memsic IRIS (Memsic, 2013).
- Micro nodes – mid-class unconstrained nodes with medium computational capabilities, embodied with a single GPP and able to run Linux kernels. They are typically DC-powered and have the potential for deployment of a large number of SPD functionalities. Examples of commercially currently available embedded platforms that correspond to the definition of Nano nodes are e.g. Beaglebone (Beagleboard, 2013c), Beagleboard (Beagleboard, 2013a) and Raspberry PI (RaspberryPiFoundation, 2013).
- Power nodes – high-class unconstrained nodes with advanced computational capabilities, typically embodied with multiple processing units and able to run high-level operating systems such as WinCE and QNX. Examples of commercially-available platforms that can be considered as power nodes are Beagleboard-xM (Beagleboard, 2013b) and ZedBoard (ZEDBoard, 2013). These nodes may further be embodied with the widely tunable RF front end, or connected to the full Software Defined Radio, making them a "SDR-capable power node".

The full set of the SPD functionalities developed for the Node layer is shown in Figure 2. Which of the functionalities are being exercised at a given time instance depends on the node class (Nano/Micro/Power) and the SPD level imposed by the Overlay.

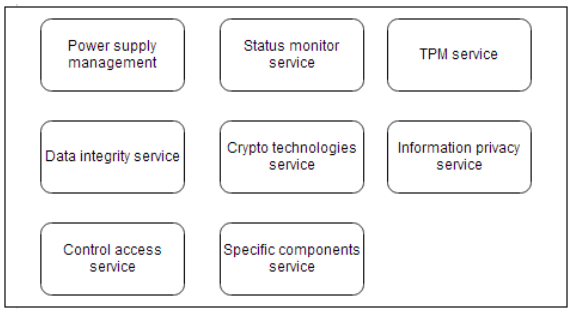

Figure 2: SPD functionalities at the Node layer.

The Network layer is a heterogeneous layer in charge of provisioning an SPD-enabled communica-

tion between two or more nSHIELD nodes and/or the external world. It is composed of a common set of cooperating protocols, procedures, algorithms and communication technologies, which are classified into four innovative features:

- SPD-driven Smart Transmission Layer – feature built specifically for the SDR-capable power nodes (unconstrained devices with high reconfigurability potentials), whose goal is ensuring reliable and robust communication in harsh and critical conditions by utilizing on-the-fly reconfigurability prospects of Software Defined Radio technology and - eventually - the learning prospects that Cognitive Radio technology brings.
- Distributed Self-x Models – a set of distributed self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks, whose goal is reducing the vulnerability to attacks depleting communication resources and node energy. This feature is not dependent upon the node class, but rather upon the network model and topology.
- Reputation-based Resource Management Technologies – when possible, keeping track of the behaviour of the network's nodes can provide significant improvements to the overall security, as it can assist in singling out continuous anomalous, malicious and unwanted behaviour. Hence, this feature (Gerrigagoitia et al., 2012) will provide efficient solutions based on trust level and reputation tracking, allowing for secure routing protocols and functional intrusion detection systems at the communication level. In centralized networks, Reputation-based RMTs will be deployed at the central entity, thus being independent of the classes of nodes that comprise the network. In addition to that, certain aspects of Reputation-based RMTs are tailored and deployed to suit each of the node types, allowing for the feature to ensure SPD provisioning (to a certain level) in distributed environments as well.
- Trusted and Dependable Connectivity – refers to the set of SPD communication protocols deployed at the network and link layer, whose focus is put on lightweight adaptations of the well-known Transport Layer Security (TLS) protocol, Datagram Transport Layer Security Protocol (DTLS) and Internet Protocol SECurity (IPsec) (Rantos et al., 2013) with its encoded version for IPv6 over Low power Wireless Personal Area Networks (6LoWPAN). In addition, this work task deals with the access control applied specifically to Smart Grid networks.

SPD functionalities developed for the Network layer are outlined in Figure 3.

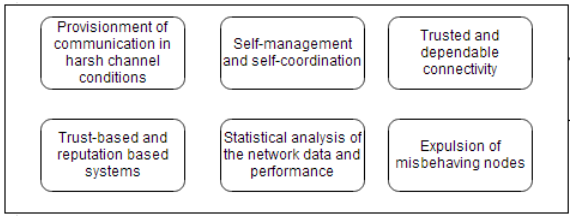

Figure 3: SPD functionalities at the Network layer.

The Middleware is a software layer installed in the nSHIELD nodes, whose complexity depends on the node class - lightweight middleware solutions are deployed for the nano nodes, and high-complex solutions for the power nodes. Middleware acts as "glue" for different SPD services offered by the nSHIELD system, as - by means of dedicated protocols, control algorithms and interfaces - it allows for the abstraction, discovery, composability and control of all of them. Middleware services and functionalities are depicted in Figure 4.

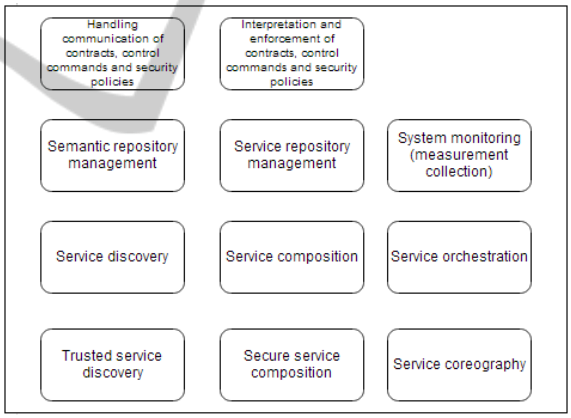

Figure 4: SPD functionalities at the Middleware layer.

The Overlay is a logical vertical layer in charge of deciding, in accordance with the control algorithms and policies, which SPD functionalities should be activated/deactivated at a given time instance, and to tailor them in order to reach the nSHIELD objectives (i.e. the desired SPD level). This layer is indeed a software routine running over the nSHIELD Middleware, which uses Middleware core services in order to collect information and actuate its decision-making process. nSHIELD Overlay offers five services, partially overlapping with the services offered by Middleware. They are depicted in Figure 5.

Validation of the concepts developed within the nSHIELD project will be demonstrated by the means of four independent scenarios/demonstrators:

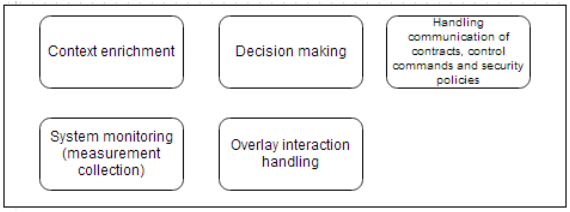

Figure 5: SPD functionalities at the Overlay layer.

- Urban railways protection
- Voice/facial recognition
- Dependable avionic systems
- Social mobility

For page limitation purposes, we are omitting a more detailed outlook on the demonstrators, and the project's ideas and methodologies as a whole. These may, however, be found at (nSHIELD Consortium, 2012), (Fiaschetti et al., 2012), (Esposito et al., 2013), (Flammini et al., 2011). The focus is instead placed on the implementational details of the SPD-driven Smart Transmission Layer, and the corresponding test bed architecture, discussed in more detail in the next section.

4 TEST BED ARCHITECTURE

The proposed Smart Transmission Layer SDR/CR test bed consists of a number (currently: 2) of Secure Wideband Multi-role - Single-Channel Handheld Radios (SWAVE HHs), each interconnected with the proprietarily developed multi-processor embedded platform (Power node).

4.1 SWAVE HH Architecture Overview

SWAVE HH (SelexES, 2013) (from now on referred to as HH) is a fully operational SDR radio terminal capable of hosting a multitude of wideband and narrowband waveforms. Maximum transmit power of HH is 5W, with the harmonics suppression at the transmit side over -50 dBc. Superheterodyne receiver has specified image rejection better than -58 dBc. The receiver is fully digital; in VHF, 12-bit 250 MHz analog to digital (AD) converters perform the conversion directly at RF, while in UHF, AD conversion is performed at intermediate frequency (IF). No selective filtering is applied before ADC. Broadband digitized signal is then issued to the FPGA, where it undergoes digital down conversion, matched filtering and demodulation.

Being a military technology, several technical characteristics of SWAVE HH, i.e. processor specifications and more in-depth operational details are non-disclosable.

HH has an integrated commercial Global Positioning System (GPS) receiver, but also provides the interface for the external GPS receiver. GPS data is available in National Marine Electronics Association (NMEA) format and may be outputted to the Ethernet port.

Radio is powered by Li-ion rechargeable batteries, however may also be externally powered through a 12.6V direct current (DC) source. Relatively small physical dimensions (80x220x50 mm), long battery life (8 hours at the maximum transmission power for a standard 8:1:1 duty cycle), and acceptable weight (960g with battery) allow for portability and untethered mobile operation of the device.

Hypertach expansion at the bottom of HH provides several interfaces, namely: 10/100 Ethernet; USB 2.0; RS-485 serial, DC power interface (max 12.7V), and PTT. The radio provides operability in both Very High Frequency - VHF (30 - 88 MHz), and Ultra High Frequency - UHF (225 - 512 MHz) band. The software architecture of the radio is compliant with the Software Communications Architecture (SCA) 2.2.2 standard. Following that, HH provides support for both legacy and new waveform types. Currently, two functional waveforms are installed on the radio: SelfNET Soldier Broadband Waveform (SBW) and VHF/UHF Line Of Sight (VU-LOS), as well as the waveform providing support for the Internet Protocol (IP) communication in accordance with MIL-STD-188-220C specification (Li et al., 1995). Currently installed waveforms will be described and analyzed in more details in section 5.2.

4.2 Power Node Architecture Overview and Connection to SWAVE HH

nSHIELD Power node is composed of a small form factor System-on-Module (SOM) with high computational power - developed by Selex ES - and the corresponding carrier board. It is based on an ARM Cortex A8 processor running at 1Ghz, encompassed with powerful programmable Xilinx Spartan 6 FPGA and Texas Instruments TMS320C64+ DSP. It can be embodied with up to 1 GB LPDDR RAM, has support for microSD card up to 32 GB, and provides interfaces for different RF front ends. Support for IEEE 802.11 b/g/n and ANT protocol standards are proffered. Furthermore, several other external interfaces are provided, i.e. 16 bit VGA interface; Mic-in, line-in and line-out audio interfaces; USB 2.0; Ethernet;

and RS-232 serial. The node is DC-powered, and has Windows CE and Linux distribution running on it. System architecture of the Power node is shown in Figure 6.

Connection to HH is achieved through Ethernet, as well as serial port. Ethernet is used for the remote control of the HH, using SNMP. For the serial connection, due to different serial interfaces - RS-232 and. RS-485, a RS-232-to-RS-485 converter is needed. Serial connection is used for transferring the spectrum snapshots from HH to Power node. More details on remote control and spectrum sensing are given in sections 5.1 and 5.4, respectively.

Figure 7: Implementations of SWAVE HH and the SOC Power node.

4.3 Assembled Test Bed

Current test bed prototype is composed of two SWAVE HHs, each interconnected with a Power node. A coaxial RF bench was implemented for the frequency range of interest. Because of the high output power of the radios, two programmable attenuators had to be included in the coaxial path, and were programmed to their maximum attenuation value - 30 dB. Agilent 778D 100 MHz - 2GHz dual directional coupler with 20dB nominal coupling was placed between the attenuators, allowing for sampling and monitoring the signal of interest. Agilent E4438C vector signal generator was connected to incident port of the coupler, with the purpose of injecting noise/interference signal to the network. Agilent E4440A spectrum analyzer was connected to the coupler's reflected port, facilitating the possibility of monitoring the RF activity. Simplified block diagram of the test bed, and implementation are shown in Figures 8 and 9 respectively.

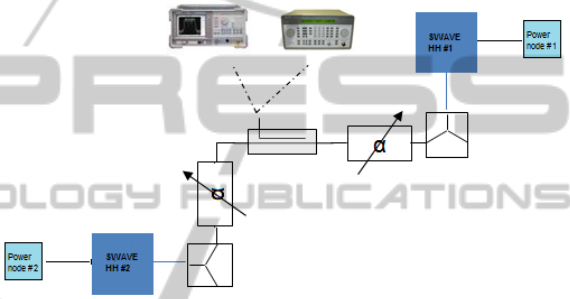

Figure 8: Test bed simplified diagram.

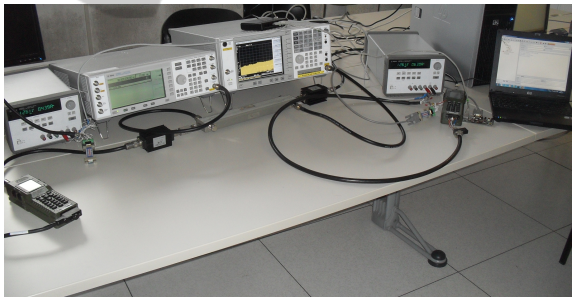

Figure 9: SPD-driven Smart Transmission Layer test bed implementation.

5 CASE STUDIES

Smart Transmission Layer based on the described test bed architecture is currently in its early implementation phase. However, several basic functionalities have already reached demonstrable level. These will be described in more details as follows.

5.1 Remote Control of the Radio

Using Simple Network Management Protocol v3 (SNMP v3), several parameters of the HH radio may

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

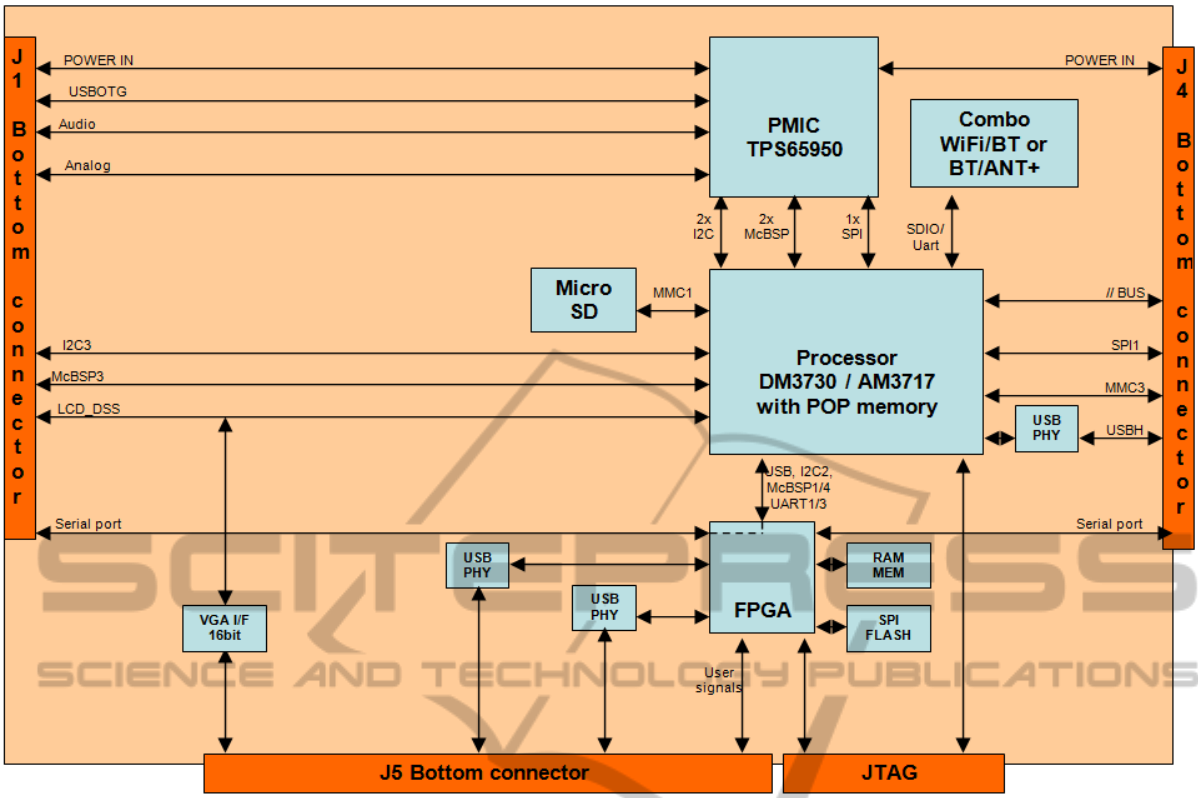

Figure 6: nSHIELD Power node - system architecture.

be externally controlled. For achieving this, SNMP manager has to be installed and running on the Power node. The host (Power node) and the agents (HHs in the network) are connected through an Ethernet hub, and need to be on the same domain.

By utilizing three basic SNMP commands: GET, SET and TRAP, it is possible to: read the current value of the parameter, set a new value, or issue a message/warning if the current value satisfies a condition, respectively.

The controllable parameters and their corresponding features are stored in a Management Information Base (MIB), which is loaded into the host's SNMP manager. MIB table contains all the definitions that define properties of the controllable parameters, and describes each object identifier (OID), which is originally a sequence of integers, with a string.

The list of the parameters that may be controlled externally, with the corresponding input data types, and the SNMP commands that may be invoked is given in Table 1. Since the parameters are self-explanatory, we are omitting a detailed description on them. ManageEngine MibBrowser Free Tool (ManageEngine, 2013) was used as the SNMP manager running on the power node.

Accordingly, Table 2 provides list of the parameters that may be TRAPped, with the short description of the conditions under which TRAPping messages are issued.

5.2 Waveform Analysis

As previously stated, there are currently two functional wavevorms installed on SWAVE HHs: SBW and VULOS. Having a wideband spectrum analyzer allows for monitoring the waveforms and analyzing their parameters.

SBW is a wideband multi-hop Mobile Ad-hoc NETwork (MANET) waveform, supporting operation in the 225 - 512 MHz part of the UHF band. The waveform provides self-(re)configurability and self-awareness of the network structure and topology, for up to 50 nodes and up to 5 hops. Furthermore, possibility of simultaneous streaming of voice and data services is provided, with prioritization for voice streaming (in case of exceeded bandwidth). Allocated channel bandwidth is adjustable - up to 5 MHz - with channel spacing of up to 2 MHz. SBW uses a fixed digital modulation technique.

Self-awareness is exercised by monitoring the network topology for changes every n seconds (monitor interval is adjustable). Two Quality of Service (QoS)

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 1: HH's Parameters that may be remotely controlled via SNMP.

Parameter	Type	SNMP commands
File Transfer Activation	string	SET/GET
File Transfer Type	string	SET/GET
FTP User Name	string	SET/GET
FTP Password	string	SET/GET
FTP Address	string	SET/GET
Login Username	string	SET/GET
Login Password	string	SET/GET
Transmit Power	integer	SET/GET
Transmitter On/Off	integer	SET/GET
Currently Installed Waveform	string seq	GET
Waveform's MIB Root	string	GET
Waveform Status [ON/OFF]	integer	SET/GET
Audio Message ID	string	SET/GET
Create New Waveform	string	SET/GET
Activate Preset	string	SET/GET
Activate Mission File	string	SET/GET
Audio Output Gain	float	SET/GET
Battery Charge Percentage	integer	GET
File Download Status	integer	GET
Trap Receiver's IP Address	string	SET/GET
Zeroize All Crypto Keys	integer	SET/GET
Crypto Key Loaded	integer	GET
System End Boot [failed/ succeeded/ in progress]	integer	GET

Table 2: HH's Parameters that may be TRAPped via SNMP.

Parameter	Description
NET Radio OK	The notification is triggered when the visibility of the radio network is acquired
NET Radio FAIL	The notification is triggered when the visibility of the radio network is lost
Critical Alarm	The notification is triggered when the HH has sustained a critical operational error
End Boot	The notification is triggered when successful boot-up of the HH has been verified
End File Download	The trap notifies end of the procedure of file download, indicating whether it was sucessful
Low Power	The notification is triggered when the battery charge falls below a pre-defined limit
Create Waveform OK	The notification is triggered when the waveform is successfully created
Create Waveform FAIL	The notification is triggered when the waveform creation has failed

monitoring mechanisms are provided: Bit Error Rate (BER) Test, and the statistics data for the transmitting/receiving side. These mechanisms are providing means for analyzing and comparing the quality of communication in regular and impaired channel conditions. More in-depth analysis of these features is presented in section 5.3.

Figure 10 shows envelope shape and properties of the SBW waveform, for the maximum signal bandwidth (5 MHz) and 1/10th of the maximum transmit power (-3 dBW), in frequency domain.

VULOS is a narrowband single-hop waveform designed for short-distance voice or data communication. It supports operation in both VHF (30-88 MHz) and UHF (225-512 MHz) frequency bands. The waveform allows for choosing between two analog modulation techniques: Amplitude Modulation (AM) and Frequency Modulation (FM), which may be configured on-the-fly, alongside with the modulation index. Channel bandwidth is adjustable up to 25 kHz, with channel spacing also adjustable up to 25 kHz. Furthermore, the VULOS waveform is able to utilize both digital and analog voice Coder-Decoders (CODECs) installed on the radio.

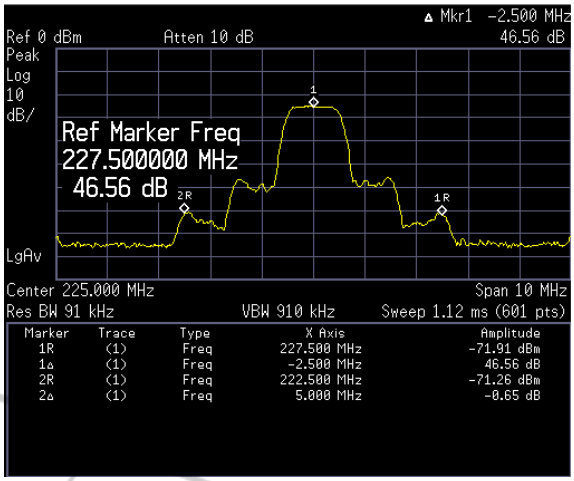

Figure 10: SBW waveform in the frequency domain - max hold.

Figure 11 shows envelope shape and properties of FM-modulated VULOS waveform with the 25 kHz bandwidth, transmitted at 1 dBW in VHF band (30 MHz).

Waveform analysis will have an important SPD application - by creating a database of waveform types that are occurring in the system, it will be possible to identify potentially malicious or misbehaving users.

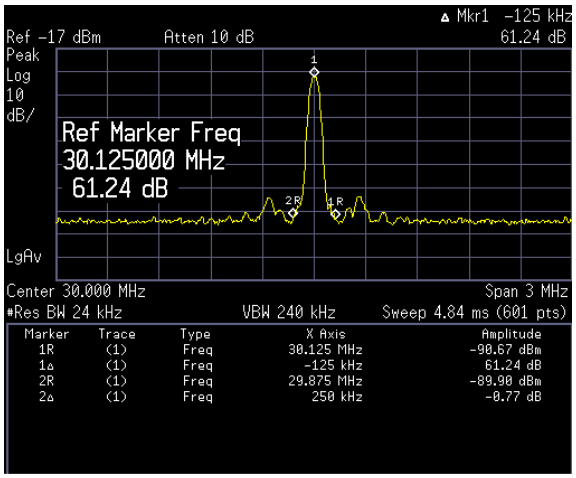

Figure 11: FM-modulated VULOS waveform in the frequency domain - max hold.

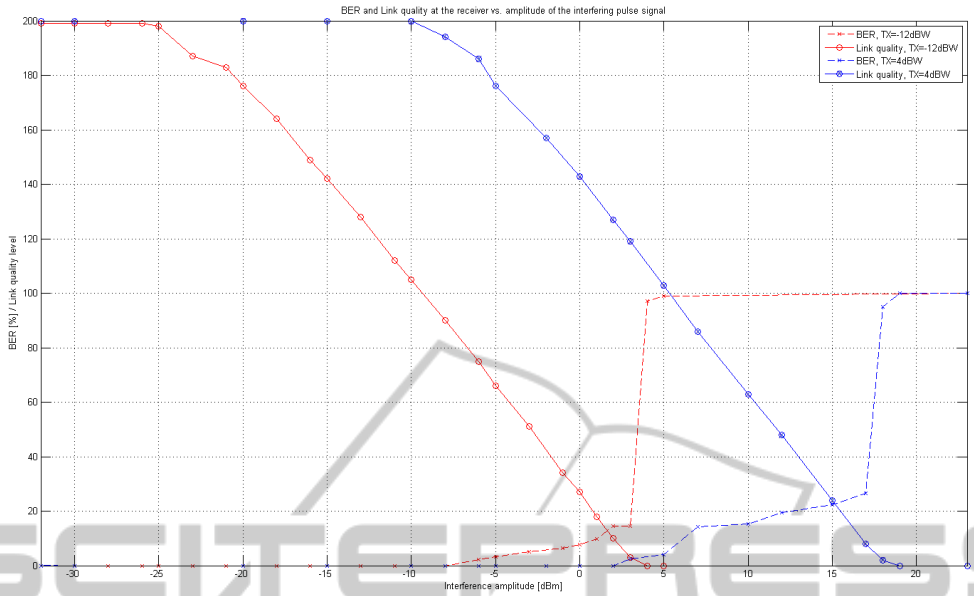

Figure 12: BER and Link quality level vs. interference amplitude of interfering pulse signal.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS

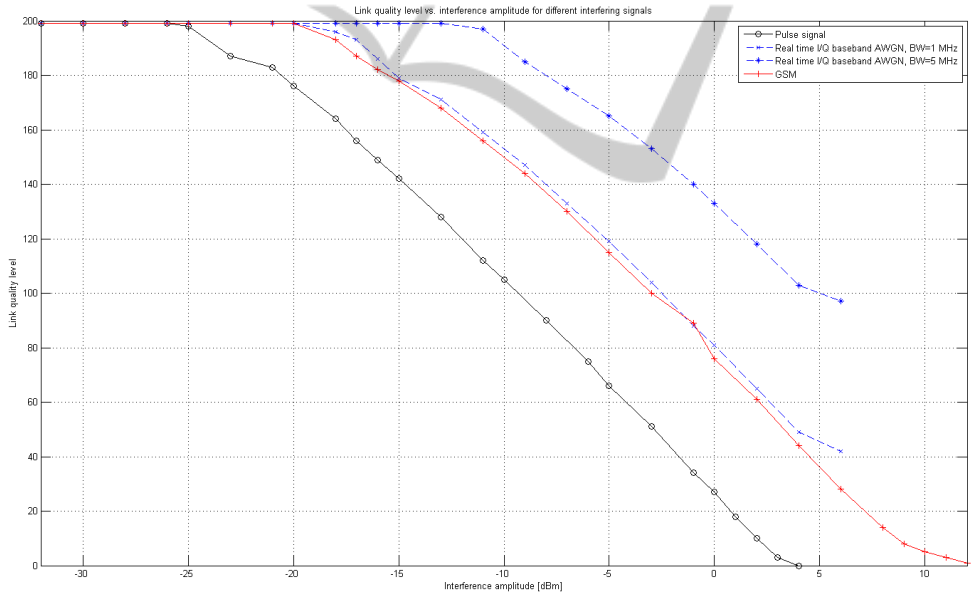

Figure 13: Link quality level vs. interference amplitude for different interfering signals.

5.3 Interference Detection

Various Denial of Service (DoS) attacks - and in particular jamming attacks - have for a long time been posing - and continue to pose - significant security threats to radio networks. Radiofrequency (RF) jamming attacks refer to the illicit transmissions of RF signals with the intention of disrupting the normal communication on the targeted channels. RF jamming is a known problem in modern wireless networks, and not an easy one to counter using traditional hardware-based equipment. Additionally, Software Defined Radios and Cognitive Radios bring the prospect for further improvement of the jamming capabilities of the malicious users, however also offer the possibility of developing advanced protection- and counter-mechanisms (Tague, 2010), (Morerio et al., 2012).

One of the main focuses of the SPD-driven Smart Transmission Layer is precisely providing safe and

reliable communication in jamming-polluted environments. For that, a detailed study of various jamming attack strategies and development of appropriate security solutions will be done.

The vector signal generator is presently used as means for creating disturbances in the communication channel, emulating a simple RF jammer. A set of measurements demonstrating how different types of created interfering signals influence the performance of the communication on the channel was done.

In the first set of measurements, the aim is to show the correlation between Bit Error Rate (BER) and the radio's built-in Link Quality metric. Link quality is HH's built-in QoS feature, and is represented by an integer in the range of [0-200]. The measurements are done with HHs having their signal bandwidths set to the maximum value (5 MHz), and repeated for two transmitting powers: -12dBW and 4 dBW. Created interfering signal is a pulse signal, created at the same frequency as the frequency of the channel used for communication between radios (225 MHz). Amplitude of the created interfering signal varies. The results are presented in figure 12.

BER percentage is shown in the first half of the Y-axis (0-100), whereas Link quality level stretches throughout the whole Y-axis (0-200). The BER curves are mutually similarly shaped, with the expected offset due to differing transmission powers of the radio. The same goes for the link quality curve shapes. As can be seen, occurrence of errors at the receiving side (area where BER>0) corresponds to Link quality levels in the range of [90-120]. As expected, 100% BER corresponds to the link quality of 0, meaning the communication has become impossible.

In the second set of measurements, different types of interfering signals are created by the signal generator, namely: pulse signal as in the first measurement set; Real Time I/Q Baseband Additive White Gaussian Noise (AWGN) with the effective bandwidth of 5 MHz; Real Time I/Q Baseband AWGN with the effective bandwidth of 1 MHz, and a GSM signal. Once again, central frequency of all of the interfering sources is the same as the frequency of the channel that the radios use for communication (225 MHz). The results are shown in figure 13.

As expected, pulse signal has the best interfering capabilities, due to the fact that it has the most concentrated power, and - importantly - that it has been created at the exact frequency as the main carrier frequency of the transmitted signal. Even with small frequency offsets, interfering impact of the pulse signal would drop significantly. For the same reason, addition of AWGN results in higher link degradation in cases of smaller allocated bandwidth, due to the higher power density. The vector signal generator is only able to produce an AWGN signal of amplitude up to 20 dBm, hence the measurements for the higher values were not done.

It should be noted that the results presented in this subsection are for reference, instead of absolute purposes - at this stage, the intention was not placed upon emulating real-life interferers, but rather at performing the initial study of the interference detection functionalities of the SWAVE HHs.

5.4 Energy Detection Spectrum Sensing

Obtaining information of the current spectrum occupancy is paramount for the Cognitive Radios to be able to opportunistically access spectrum, but may also aid them in recognizing anomalous or malicious activity by comparing the current state to those stored in their databases. There are three established methods for CRs to acquire knowledge of the spectrum occupancy: spectrum sensing (Axell et al., 2012), geolocation/database (Gurney et al., 2008), and beacon transmission (Lei and Chin, 2008). HH has a capability of performing energy detection spectrum sensing.

Every 20 seconds, 8192 samples from the ADC are transmitted over the RS-485 port - this is a functionality hard-coded in the HH's FPGA. Each sample is transmitted in two bytes: first byte containing the 6 most significant bits (MSBs), with 2 bits sign extension on the left. Second byte contains the 8 LSBs. In total, 16384 characters are transmitted, making up for the interpretation of a 16-bit word. Currently, there is not a synchronization pattern - however the idle interval between the two transmissions may be used to e.g. perform analysis of the received data. Transmission of a full window takes approximately 2 minutes.

The signal at the HH's FPGA input is a sample of raw spectrum. Raw samples are stored in a RAM buffer internal to the FPGA, and output through HH's fast serial port to the Power node, where they can be processed.

Due to the high speed of the ADC (250 MHz), serial port speed (38400 bit/s is supported in the asynchronous mode) is not sufficient for the true real-time transfer; in addition - processing capabilities of the Power node would be completely devoted to the processing of received signal, leaving no room for higher level applications. Power consumption would be heavily affected as well.

Adopted solution is to perform a quasi-real-time acquisition, i.e. to collect a large snapshot of incoming spectrum, i.e. tens of kilo-samples, and to transfer the snapshot to the Power node. When the snapshot

has been transferred, a new collection may start. This is sufficient for proper analysis of the majority of RF scenarios: in practice, only fast pulsed signals might be completely missed.

Future hardware enhancements might make real-time spectrum acquisition possible.

6 CONCLUSIONS AND FUTURE WORK

The paper has introduced concept and basic premises of the SPD-driven Smart Transmission Layer, and has described design details of test bed architecture that will be used for its development, experimentation and validation. Several case studies were performed using the test bed, demonstrating its basic capabilities. Each of these capabilities needs to be studied and developed in more detail. Following that, future work using the test bed will cover multiple topics, described as follows.

From the security perspective, the near-future work will focus on tackling the problems of advanced and intelligent DoS jamming attacks in CRNs. Using software packages such as 33503A BenchLink Waveform Builder Pro in combination with the vector signal generator, it will be possible to model various interfering attack strategies, and the appropriate counter-strategies. Because of a variety of possible attacks and potential security breaches that Software Defined Radio and Cognitive Radio technology bring, provisioning the ultimate security, privacy and dependability for SDR and CR systems is a challenging task. Addressing each of the identifiable security threats separately, though, makes for a good starting point towards achieving it.

The test bed itself will be embodied with another HH + power node, with the corresponding auxiliaries, allowing for examining more complex scenarios and creating different network topologies.

Opportunistic spectrum access is inarguably one of the most exciting features of prospective Cognitive Radio Systems. Building upon the HH's possibility of acquiring the spectrum occupancy information through energy detection, briefly presented in this paper, we aim at developing algorithms for spectrum intelligence - as the prerequisite for OSA.

Theoretical foundations for the nSHIELD framework were also described in the paper. However, common hardware and software interfaces of SPD-driven Smart Transmission Layer to the upper nSHIELD layers - Middleware and Overlay - still need to be decided upon in the future. Also, layers' interdependability will need to be looked into more closely. Hence, for the time being, the nSHIELD Middleware and Overlay layers are being treated as "black boxes".

ACKNOWLEDGEMENTS

This work was developed within the nSHIELD project (http://www.newshield.eu) co-funded by the ARTEMIS JOINT UNDERTAKING (Subprogramme SP6) focusing on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

The authors would like to thank Selex ES and Sistemi Intelligenti Integrati Tecnologie (SIIT) for providing the equipment for the test bed, and the laboratory premises for the test bed assembly. Particular acknowledgment goes to Virgilio Esposto of Selex ES, for providing expertise and technical assistance.

REFERENCES

Arduino (2013). Arduino uno datasheet. http://arduino.cc/en/Main/arduinoBoardUno.

Axell, E., Leus, G., Larsson, E., and Poor, H. (2012). Spectrum sensing for cognitive radio : State-of-the-art and recent advances. *Signal Processing Magazine, IEEE*, 29(3):101–116.

Beagleboard (2013a). Beagleboard system reference manual. http://beagleboard.org/static/BBSRM_latest.pdf.

Beagleboard (2013b). Beagleboard xm system reference manual. http://beagleboard.org/static/BBxMSRM_latest.pdf.

Beagleboard (2013c). Beaglebone system reference manual. http:// beagleboard.org/ static/ beaglebone/ latest/ Docs/ Hardware/ BONE_SRM.pdf.

Cabric, D., Tkachenko, A., and Brodersen, R. W. (2006). Experimental study of spectrum sensing based on energy detection and network cooperation. In *Proceedings of the first international workshop on Technology and policy for accessing spectrum*, TAPAS '06, New York, NY, USA. ACM.

Dabcevic, K., Marcenaro, L., and Regazzoni, C. S. (2013). Security in cognitive radio networks. In T. D. Lagkas, P. Sarigiannidis, M. L. and Chatzimisios, P., editors, *Evolution of Cognitive Networks and Self-Adaptive Communication Systems*, pages 301–333. IGI Global.

Esposito, M., Fiaschetti, A., and Flammini, F. (2013). The new shield architectural framework. *ERCIM News*, 2013(93).

Farrell, R., Sanchez, M., and Corley, G. (2009). Software-defined radio demonstrators: An example and future trends. *Int. J. Digital Multimedia Broadcasting*, 2009.

Fette, B. A. (2006). *Cognitive radio technology*. Newnes/ Elsevier.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Fiaschetti, A., Suraci, V., and Delli Priscoli, F. (2012). The shield framework: How to control security, privacy and dependability in complex systems. In *Complexity in Engineering (COMPENG), 2012*, pages 1–4.

Flammini, F., Bologna, S., and Vittorini, V., editors (2011). *Computer Safety, Reliability, and Security - 30th International Conference, SAFECOMP 2011, Naples, Italy, September 19-22, 2011. Proceedings*, volume 6894 of *Lecture Notes in Computer Science*. Springer.

Fragkiadakis, A., Tragos, E., and Askoxylakis, I. (2013). A survey on security threats and detection techniques in cognitive radio networks. *Communications Surveys Tutorials, IEEE*, 15(1):428–445.

Gerrigagoitia, K., Uribeetxeberria, R., Zurutuza, U., and Arenaza, I. (2012). Reputation-based intrusion detection system for wireless sensor networks. In *Complexity in Engineering (COMPENG), 2012*, pages 1–5.

Gurney, D., Buchwald, G., Ecklund, L., Kuffner, S., and Grosspietsch, J. (2008). Geo-location database techniques for incumbent protection in the tv white space. In *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, pages 1–9.

Lei, Z. and Chin, F. (2008). A reliable and power efficient beacon structure for cognitive radio systems. *Broadcasting, IEEE Transactions on*, 54(2):182–187.

Li, H., Amer, P. D., and Chamberlain, S. C. (1995). Estelle specification of mil-std 188-220 datalink layer - interoperability standard for digital message transfer device subsystems. In *Proceedings of MILCOM '95*.

ManageEngine (2013). Mibbrowser free tool faq. http://www.manageengine.com/products/mibbrowser-free-tool/faq.html.

Memsic (2013). Memsic iris datasheet. http://www.memsic.com/ userfiles/ files/ Datasheets/ WSN/ IRIS_Datasheet.pdf.

Minden, G., Evans, J., Searl, L., DePardo, D., Petty, V., Rajbanshi, R., Newman, T., Chen, Q., Weidling, F., Guffey, J., Datla, D., Barker, B., Peck, M., Cordill, B., Wyglinski, A., and Agah, A. (2007). Kuar: A flexible software-defined radio development platform. In *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pages 428–439.

Mitola, J. and Maguire, G. Q. Jr. (1999). Cognitive radio: making software radios more personal. *Personal Communications, IEEE*, 6(4):13–18.

Morerio, P., Dabcevic, K., Marcenaro, L., and Regazzoni, C. (2012). Distributed cognitive radio architecture with automatic frequency switching. In *Complexity in Engineering (COMPENG), 2012*, pages 1–4.

nSHIELD Consortium (2012). New shield. http://www.newshield.eu/.

Rantos, K., Papanikolaou, A., and Manifavas, C. (2013). Ipsec over ieee 802.15.4 for low power and lossy networks. In *Proceedings of the 11th ACM International Symposium on Mobility Management and Wireless Access*, MobiWac '13, pages 59–64, New York, NY, USA. ACM.

RaspberryPiFoundation (2013). Raspberry pi home page. http://www.raspberrypi.org/.

SelexES (2013). Swave hh specifications. http://www.selexelsag.com/internet/localization/IPC/media/docs/SWave-Handheld-Radio-v1-2012Selex.pdf.

Tague, P. (2010). Improving anti-jamming capability and increasing jamming impact with mobility control. In *Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on*, pages 501–506.

Tkachenko, A., Cabric, D., and Brodersen, R. (2006). Cognitive radio experiments using reconfigurable bee2. In *Signals, Systems and Computers, 2006. ACSSC '06. Fortieth Asilomar Conference on*, pages 2041–2045.

ZEDBoard (2013). Zedboard quick start. http://www.zedboard.org/sites/default/files/documentations/GSC-AES-Z7EV-7Z020-G-v1f-press.pdf.

Zolertia (2013). Zolertia z1 revc datasheet. http://zolertia.sourceforge.net/wiki/mages/e/e8/Z1_RevC_Datasheet.pdf.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS