Document No.	Security Classification	Date
/nSHIELD/SE/D4.1/A	CO	31.05.2012

Project no: 269317

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

Instrument type: Capability Project

Priority name: Embedded Systems

SPD Networks Technologies Assessment

For the nSHIELD-project

Deliverables D4.1 Revision B

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)	
CO	Confidential, only for members of the consortium (including the Commission Services)	x

Document Authors and Approvals

Authors		Date	Signature
Name	**Company**		
Krešimir Dabčević	UNIGE	**13/04/12**	
Carlo Regazzoni	UNIGE	**19/04/12**	
Marco Cesena	SELEX Elsag	**19/04/12**	
Iñaki Eguia	Tecnalia	**19/04/12**	
Roberto Uribeetxeberria	MGEP	**01/05/12**	
Iñaki Arenaza	MGEP	**01/05/12**	
Reviewed by			
Name	**Company**		
Marco Cesena	SELEX Elsag S.p.A.		
Elisabetta Campaiola	SELEX Elsag S.p.A.		
Approved by			
Name	**Company**		
Elisabetta Campaiola	SELEX Elsag S.p.A.		

Applicable Documents

ID	Document	Description
[01]	TA	nSHIELD Technical Annex

Modification History		
Issue	**Date**	**Description**
Draft A	28.03.2012	First ToC
Draft B	24.05.2012	Partners contribution
Rel 1.2	31.05.2012	Revised

Contents

Figures

Acronyms

ADSP	Attack-tolerant Distributed Sensing Protocol
BER	Bit Error Rate
BF	Beacon Falsification
CCC	Common Control Channel
CPDF	Conditional Probability Density Function
CR	Cognitive Radio
CRN	Cognitive Radio Network
CWSN	Cluster Wireless Sensor Networks
DRBTS	Distributed Reputation and trust-based Beacon Trust System
ESs	Embedded Systems
FC	Fusion Center
FCC	Federal Communications Commission
FPGA	Field Programmable Gate Array
HIDS	Host Intrusion Detection System
HLR	High Level Requirements
IDS	Intrusion Detection System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	Internet Protocol Security
LSSL	Light Secure Socket Layer
NIDS	Network Intrusion Detection System
NPHCT	Neyman-Pearson Composite Hypothesis Testing

PDF	Probability Density Function
PU	Primary User
PUEA	Primary User Emulation Attack
R-CFG	Radio Configuration
RBFC	Random Branch Function Call
RFSN	Reputation-based Framework for Sensor Network
RSS	Received Signal Strength
SBW	Small Backoff-Window
SDR	Software Defined Radio
SNR	Signal to Noise Ratio
SRM	Secure Radio Middleware
SRS	System Requirements and Specification
SSDFA	Spectrum Sensing Data Falsification Attack
SSL	Secure Socket Layer
SOA	Service-oriented Architecture
SPD	Security Privacy Dependability
SU	Secondary User
QoS	Quality of Service
TCP	Transmission Control Protocol
WO	Wireless Operator
WSN	Wireless Sensor Network
WSPRT	Wald’s Sequential Probability Ratio Test

1 Executive Summary

At the start-up of the project, an assessment is done on the technologies that the pSHIELD project has examined, in order to full address the innovative technologies for the nSHIELD project.

In the following section the technologies examined in the nSHIELD project are described.

Part of these technologies were examined partially in pSHIELD project, nSHIELD will complete the identification of these technologies, will identify additional technologies and will explore in detail the technologies that will be classified like the more suitable to add SPD to the communication networks based on the Embedded Systems.

2 Introduction

2.1 The nSHIELD System

nSHIELD is a project co-funded by the ARTEMIS JOINT UNDERTAKING (Sub-Programme SP6) focused on the research of SPD (Security, Privacy, Dependability) in the context of Embedded Systems.

The nSHIELD project is, at the same time, a complement and significant technology breakthrough of pSHIELD, a pilot project funded in ARTEMIS Call 2009 as the first investigation towards the realization of the SHIELD Architectural Framework for Security, Privacy and Dependability (SPD).

The roadmap, already started in the pilot project, will bring to address SPD in the context of Embedded Systems (ESs) as “built in” rather than as “add-on” functionalities, proposing and perceiving with this strategy the first step toward SPD certification for future ES.

pSHIELD has covered the definition phase of this roadmap: nSHIELD will be in charge of the development and implementation phases. The SHIELD General Framework consists of four layered system architecture and Application Layer in which four scenarios are considered:

- Railway
- Voice/Facial Recognition
- Dependable Avionic Systems and
- Social Mobility and Networking.

The leading concept is to demonstrate composability of SPD technologies. Starting from current SPD solutions in ESs, the project will develop new technologies and consolidate the ones already explored in pSHIELD in a solid basement that will become the reference milestone for a new generation of ”SPD-ready” ESs.

nSHIELD will approach SPD at 4 different levels: node, network, middleware and overlay. For each level, the state of the art in SPD of individual technologies and solutions will be improved and integrated (hardware and communication technologies, cryptography, middleware, smart SPD applications, etc.).

The SPD technologies will be then enhanced with the “composability” functionality that is being studied and designed in pSHIELD, in order to fit in the SHIELD architectural framework.

The composability of this architectural framework will have great impact on the system design costs and time to market of new SPD solutions in ESs.

At the same time, the integrated use of SPD metrics in the framework will have impact on the development cycles of SPD in ESs because the qualification, (re-) certification and (re-)validation process of a SHIELD framework instance will be faster, easier and widely accepted.

2.1.1 Security Concept

When addressing the security concept, an additional attribute has great prominence: confidentiality, i.e. the absence of unauthorized disclosure of information.

Security is a composite of the attributes of confidentiality, integrity (in the security context, “improper” means “unauthorized"), and availability (for authorized actions only).

Integrity and availability are two competing dependability/security attributes. While some applications require strict integrity, other applications exist, e.g., safety or mission critical systems, where - depending on the specific situation - availability is more important for dependability than strict integrity.

Within our work, we focus on data-centric systems, where availability can be increased by temporarily relaxing data integrity, thereby allowing for certain inconsistencies.

Potential inconsistencies are accepted based on constraint validation on replicated copies that are possibly stale in the face of network partitions.
Such consistency threats need to be bound and eventually resolved during reconciliation to re-establish a consistent system state.

The integrity of data means its accuracy and completeness. Data have integrity if they have not been corrupted in any way.

In information security, integrity means that data cannot be modified undetectably. Integrity is violated when a message is actively modified in transit.

Most cipher systems provide message integrity along with privacy as part of the encryption process. Messages that have been tampered with in flight will not be successfully decrypted.

Integrity means assurance that the information is authentic and complete. The term “Integrity” is frequently used when considering Information Security, as it represents one of the primary indicators of security (or lack of it).

The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. For example, making copies (say by e-mailing a file) of a sensitive document, threatens both confidentiality and the integrity of the information.
Why? Because, by making one or more copies, the data is at risk of change or modification.

Availability is the area of information security that requires services and components to be continuously available for the user community. If a service or component is unavailable, confidentiality and integrity are meaningless.

Network availability is the underlining attribute that must be existent in order to guarantee that services are accessible for end users.

For any information system to serve its purpose, the information must be available when it is needed.

This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it, must be correctly functioning. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Ensuring availability also involves preventing denial-of-service attacks.

2.1.2 Privacy Concept

Privacy is almost a stand-alone concept with no specific attributes. As far as the “privacy” concept is concerned, the definition of privacy arrives from Latin: *privatus* - "separated from the rest, deprived of something, esp. office, participation in the government", from *privo* - "to deprive".

It refers to the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes.

Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something within them that is considered inherently special or personally sensitive.

The degree to which private information is exposed therefore depends on how the public will receive this information, which differs between places and over time.

Privacy is broader than security and includes the concepts of appropriate use and protection of information.

Therefore, the pSHIELD scenario should define clearly how privacy enters in the transportation of dangerous materials: in case no specific privacy issues will be identified, then the concept of privacy will be covered by the most adequate “confidentiality” (see following section).

2.1.3 Dependability Concept

Dependability is a composite concept that encompasses the following attributes:

- Availability: readiness for correct service
- Reliability: continuity of correct service
- Safety: absence of catastrophic consequences on the user(s) and the environment
- Integrity: absence of improper system alterations
- Maintainability: ability to undergo modifications and repairs

Dependability of a structural system is a comprehensive concept that - by definition - describes the quality of the system as its ability to perform as expected in a way that can be justifiably trusted.

One of the attributes of dependability is integrity, which can be interpreted as the absence of improper alterations of the structural configuration.

The assessment of the integrity during the whole life-cycle can be carried out efficiently by implementing a monitoring system able to detect and diagnose any fault at its onset.

Availability refers to the accessibility of the system to users. A system is available if its users' requests for service are accepted at the time of their submission. Unlike reliability, availability is instantaneous.

The former focuses on the duration of time a system is expected to remain in continuous operation – or effectively so in the case of recovery-enhanced reliability - starting in a normal state of operation. The latter concentrates on the fraction of time instants where the system is operational in the sense of being accessible to the end user.

Based on the above considerations, it is clear that in some cases integrity and availability are more security oriented, whilst in other cases these two attributes are more related to dependability. So, in the former cases, these attributes will be dealt with in the security section, whilst, in the latter cases, in the dependability section.

2.1.4 Fault-Tolerance Concept

Threats include faults, errors and failures, as well as their causes, consequences and characteristics. An error is defined as the part of a system's total state that may lead to a failure.

A service failure occurs when an error causes the delivered service to deviate from correct service.

The cause of an error is called a fault: a fault may arise from physical imperfections in the system, physical influence and damage from the outside, human logical faults made during specification, design, development, installation and operation, etc.

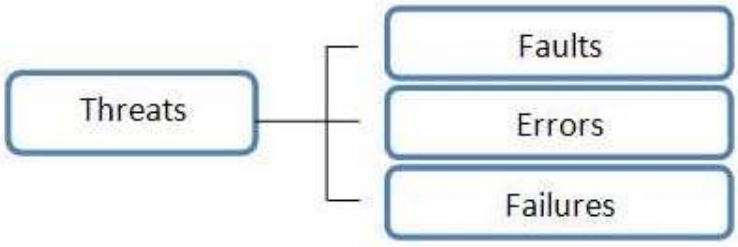

Figure 1: Threats classification

Many means have been developed to attain the various attributes of dependability and security. Those means can be grouped into four major categories:

- Fault prevention means to prevent the occurrence or introduction of faults
- Fault tolerance means to avoid service failures in the presence of faults
- Fault removal means to reduce the number and severity of faults
- Fault forecasting means to estimate the present number, the future incidence, and the likely consequences of faults

In the scope of the project, nSHIELD could be considered as the system in charge of the maintenance of SPD properties.

This is summarized in the following figure:

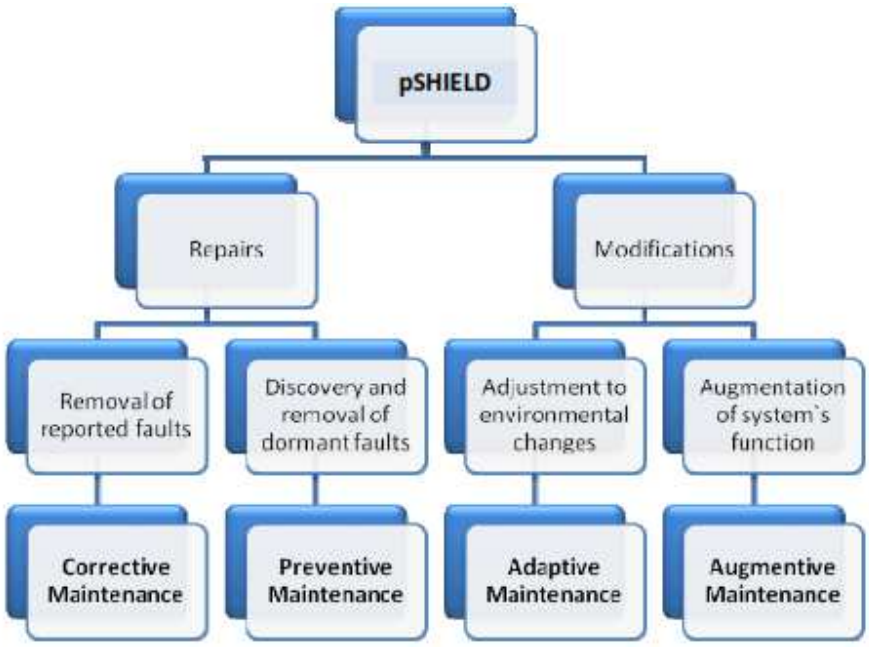

Figure 2: Actions to preserve SPD

It is noteworthy that repair and fault tolerance are related concepts; the distinction between fault tolerance and maintenance in this paper is that maintenance involves the participation of an external agent, e.g., a repairman, test equipment, remote reloading of software.

Furthermore, repair is part of fault removal (during the use phase), and fault forecasting usually considers repair situations.

In fact, repair can be seen as a fault tolerance activity within a larger system that includes the system being repaired and the people and other systems that perform such repairs.

2.1.5 Reputation-based Concept

Reputation based concept is non deterministic attribute for a particular nSHIELD element. Reputation will be used in nSHIELD both for preventive and corrective phases.

Reputation is the concept for measuring the trustworthy parameter/principal for an external or unknown element that desires to interact with nSHIELD project.

There many mechanism for developing reputation-based mechanism in network layer.

The main rule for this is to establish communication channels between different nodes in order to establish a secure conversation protocol and determine if this element is the appropriate one to interact with.

These mechanisms enable heterogeneity and interoperability across multiples systems and sub-systems but some new risk emerge because of permitting interfaces with external elements (i.e. legacy systems or interfaces to new emerging technologies)

In the following sections some of these mechanisms will be described.

2.1.6 Intrusion Detection

Intrusion detection systems (IDS) can be defined as a set of different scanners that monitor the activities of an information system looking for malicious actions. An IDS is not an antivirus designed to detect malware or a first line barrier like firewall, it is a detection system that identifies anomalous activities, alerts about them and optionally takes reactive actions to subsane them.

We can classify the different kind of existing IDS based on the following criteria:

- Host-based versus Network-based: The IDS agents can be installed inside hosts, and they run apart from the normal functionalities of host, monitoring the activities inside the host. These are called Host intrusion detection system (HIDS).

  Instead in Network intrusion detection system(NIDS), the agents are installed in special devices and monitor the network traffic. Usually these devices are completely transparent for the network because they do not answer to any link layer or network layer addresses, i.e., they operate as passive devices. If they need to communicate with reporting or management systems, they usually have a second link to a different network (the management network).

- Centralized versus Decentralized: In centralized IDS there is an agent that collects and analyzes all the anomalous activities of the whole system and sends alerts or takes actions depending on the result the analysis.

  On the other hand, decentralized IDS are composed of several agents that run independently and collect and analyze their own anomalous activities, taking their own mesasures. This type of IDS is more resistant and versatile, but also more complicated to configure and maintain.

- Type of analysis used to detect anomalous activities: In misuse-based analysis the IDS agent compares the data from the monitored system with known malicious patterns stored in its attack database. If it finds a match it will raise an alarm (an optionally adopt a counter measure). On the other hand, in anomaly-based analysis the IDS agent compares the monitored system activity with the normal behaviour that it is supposed to have (this normal behaviour is usually modelled beforehand).

In the scope of the project, the IDS will be the first safety barrier for possible attacks against the system, warning of possible attacks to maintain reliability and availability of the network.

3 SPD High Level Requirements for nSHIELD System

3.1 nSHIELD System

3.1.1 nSHIELD Network

This chapter provides assessment of the technologies for SPD in embedded systems focusing on the Network layer, that have previously been studied within the pSHIELD project (see public deliverable 4.2 “SPD Network technologies prototype report”), as well as alternative technologies that have not been examined within the pSHIELD project.

Having decided that the implementation of the Smart Transmission Layer is to rely on the Software Defined Radio (SDR) platform which - once equipped with the possibilities of maintaining scenario awareness, detecting possible threats and adapting to the new situations by itself – will evolve towards the Cognitive Radio (CR), the common threats regarding SPD for these systems (SDRs and CRs) will be presented.

Overview of the proposed countermeasures and solutions for those threats will then be given. Furthermore, the basic ideas of the self-management and self-coordination schemes for unmanaged and hybrid managed/unmanaged networks will be explained.

The ultimate goal is to come up with the set of solutions that will integrate all of the relevant mechanisms for ensuring SPD in the SDR-based and CR-based embedded systems.

3.1.1.1 SPD in SDRs

Smart SPD information transmission (see pSHIELD deliverable 4.1. “SPD Network technologies prototype”) is a feature of the nSHIELD system – introduced previously in the pSHIELD project – based on a Network Layer Service, usually called Software Defined Radio (SDR).

There is no unanimous definition of the SDR – however, one of the most recognizable, and in the same time very intuitive ones is Wireless Innovation Forum’s one, which recognizes SDR as “a radio in which some or all of the physical layer functions are software defined”.

These functions usually include - but are not limited to - frequency; modulation technique; cryptography; used bandwidth, coding technique, etc. However, the level of reconfigurability/reprogrammabillity needed for the radio to be classified as a SDR isn’t strictly defined.

The “ideal” SDR would, therefore, have all of the radio-frequency bands and modes defined in software.

Some of the major security concerns from the perspective of a mobile appliance are:

- *User identification* attempts to ensure that only authorized entities can use the appliance.
- *Secure storage* addresses the security of sensitive information such as passwords, PINS, keys, certificates, etc., that may reside in secondary storage (e. g., flash memory) of the mobile appliance.
- A *secure software execution environment* is necessary to ensure that attacks from malicious software such as viruses or trojan horses are prevented.

- A *tamper-resistant system implementation* is required to ensure security of the hardware implementation from various physical and electrical attacks.

- *Secure network access* ensures that only authorized devices can connect to a network or service.

- *Secure data communications* considers the privacy and integrity of data communicated to/from the mobile appliance.

- *Content security* refers to the problem of ensuring that any content that is downloaded or stored in the appliance is used in accordance with the terms set forth by the content provider (e. g. read only, no copying, etc.).

Several requirements were imposed on the network layer in the pSHIELD project, which transcribe to nSHIELD as well. (from pSHIELD deliverable 2.1.2. “System Requirements and Specifications”). Namely, it is stated that the network layer:

- shall be secure

- should have suitable security protocols

- should support security protocols to protect entire IP payload or upper-layer protocols

- should provide Availability, Confidentiality and Integrity

- shall support anti-replay protection to prevent against a denial of service attack

- shall support data confidentiality to protect, and to encrypt the entire data

- shall support algorithms for encryption

- shall support data integrity to ensure that the contents of the packet do not change in transit

- shall support data authentication to verify that the packet received is actually from the claimed sender

- should use the IPSec protocol

- should support more efficient algorithms for fast and better speed of execution to satisfy the conditions in the case of limited processing and power capabilities of embedded devices

- should support symmetrical cryptography

- should provide dependability mechanism

- should provide Reliability, Availability, Safety, Maintainability, and Integrity

- should provide privacy

Ensuring SPD for SDR systems involves dealing with two main issues: software-based protection and hardware-based protection.

Software-based protection schemes involve the deployment of tamper-resistance techniques to defend against malicious or buggy software installations.

These schemes also involve techniques and algorithms for the secure download and distribution of software into several SDRs.

As CRNs have to be flexible, updated software can be frequently downloaded from servers through the Internet. Secure downloading involves mechanisms that protect the integrity of the data exchanged, protect against eavesdropping, as well as providing secure authentication between the communication parties.

Hardware-based protection schemes include modules implemented in hardware acting as isolation layers between hardware and the software components.

These modules monitor several parameters of the SDR (e.g. transmission power).[5]

Several SPD mechanisms have been proposed in the literature, namely:

- Light Secure Socket Layer (LSSL) by Brawerman et al. [6] - a lightweight protocol based on the SSL protocol, but takes up less bandwidth, thus, it is more suitable for SDR handheld devices operating under low-capabilities, low-bandwidth and error-prone wireless links.

  However, securing the radio configuration (R-CFG) download connection does not guarantee that a valid radio configuration, that is, a R-CFG that has been approved by the regulatory agency, has been downloaded. In order to install only valid R-CFGs, a secure download protocol is presented.

  The secure protocol includes, besides the LSSL, steps of mutual authentication, public/private key mechanisms for data encryption and decryption, and fingerprint calculations to check data integrity.

  Finally, the secure protocol is analyzed and shown to be deadlock and livelockfree, and to properly terminate.

- Uchikawa et al. [7] - a secure download system which uses the characteristics of the field programmable gate arrays (FPGAs) composing the SDR.

  The proposed system has the novelty that realization of high security enciphering is possible. This is achieved using the characteristic of FPGAs which allows systems to be arranged in a variety of different layouts, as well as by using the configuration information as the key.

  This unifies the renewal of the key and the enciphering. In addition the proposed system has the merit that it has high security against illegal acquisition such as a wiretapping, and can also be used in conjunction with any other current cipher algorithm.

- Li et al. [8] - a hardware-based method where the maximum transmission power is computed and controlled by a module implemented at the hardware level of the SDR transceiver.

  The advantage is that the module, which estimates the maximum transmission power, is isolated from the software layers, which can either be compromised more easily by attackers or malfunction due to software bugs.

  The authors assume that SUs access the spectrum in an overlay approach; thus secondary and primary transmissions can take place at the same time.

- Secure Radio Middleware (SRM) Layer by Li et al. [5] - based on robust separation of the radio operation environment and user application environment through the use of virtualization.

  A secure radio middleware layer is used to intercept all attempts to re-configure the radio, and a security policy monitor checks the target configuration against security policies that represent the interests of various parties.

  Therefore, secure re-configuration can be ensured in the radio operation environment even if the operating system in the user application environment is compromised.

- Xiao et al. [9] - a tamper resistance scheme that utilizes code encryption and branch functions to alter the target program, while enabling the program to satisfy its performance requirements.

  The scheme employs a technique called the Random Branch Function Call (RBFC), which enables a user to control the tradeoff between integrity checking frequency and the overhead, and consists of two phases: (i) transformation where the unprotected assembly code becomes tamper-resistance protected offline, and (ii) verification where a code is checked for integrity violations.

  The proposed scheme is designed to thwart static attacks (static information extracted by examining the software code) and to protect partially against dynamic attacks (dynamic information extracted while the software code executes).

- Brawerman et al. [10] - a framework for cloning prevention of SDR Mobile Devices. It provides a set of software and hardware technologies that along with the cooperation of a Wireless Operator (WO) can prevent cloning.

  Unlike other schemes, the proposed anti-cloning framework not only detects cloned units, but also elevates the level of difficulty to clone a valid unit.

  The WO in this contribution is assumed to be the manufacturer of the SDR. The cooperation is performed through an authentication process where the WO verifies that the specific SDR is the original and not a cloned one.

The framework is independent of the wireless communication technology, working well for different cellular technologies and the Internet.

3.1.1.2 SPD in CRNs

Although this doesn't necessarily have to be the case, Cognitive Radio is usually defined as an upgraded SDR in the sense that it is self-reconfigurable and has learning capabilities, i. e. the radio can reconfigure itself through an ongoing process of awareness (both of itself and the outside world), perception, reasoning, and decision making.

However, because of those two traits (cognitive capability and reconfigurability), CR technology has also raised new threats and vulnerabilities (in addition to common threats present in traditional wireless networks AND the aforementioned SDR-specific threats).

Security is necessary in CRNs because the data channel is easily accessed by an attacker. In the context of CRNs, we define attacks as actions that achieve at least one of the following goals:

- Unacceptable interference to licensed primary users: Because of the attack, the communication channel of primary/licensed users of a frequency band is diminished or just becomes unusable (denial-of-service (DoS) attack).

- Missed opportunities for secondary users: An attacker could prevent secondary users from using available spectrum bands thus, once again, reducing channel performance or just denying service to secondary users.

- Access to private data: An attacker could try to access data in an unauthorized way. As a consequence, data must be secured by means of cryptographic primitives.

- Modification of data: An attacker could try to modify the data exchanged between several entities to its own advantage. Thus, integrity of data must be assured.

- Injection of false data: Injection of false data could make the CRN to perform in an unpredictable way or just following the attacker guidelines. Therefore, authentication of information sources should be guaranteed.

Hence, it is possible to divide CR-specific attacks with regard to what the attacker is trying to achieve, as well as which layer he is targeting. We have:

- Primary User Emulation Attacks (PUEAs)

- Spectrum Sensing Data Falsification Attacks (SSDFAs)

- Beacon Falsification (BF) attack

- Small Backoff-Window (SBW) attack

- Lion attack

3.1.1.2.1 Primary user emulation attacks

Primary user emulation attack (PUEA) is first identified by Chen and Park in 2006. In PUEA, an attacker occupies the unused channels by emitting a signal with similar form as the primary user's signal so as to deter the access of the vacant channels from other secondary users.

The cognitive radios have highly reconfigurable air interface which makes it possible for an attacker to modify the air interface to mimic a primary user signal's features and thereby leading legitimate secondary users to erroneously identify the attacker as a primary user.

The investigation shows that a PUE attacker can severely compromise the spectrum sensing performance and significantly reduce the channel availability to legitimate secondary users.

PUEA can compromise a cognitive radio system using either of spectrum sensing methods to attack the energy detection scheme, PUE attacker may masquerade the primary user by transmitting signal with the similar energy as primary user; to defeat cyclostationary detectors, an attacker can make its transmissions indistinguishable from primary user signals by transmitting signals that have the same cyclic spectral characteristics as primary user signals.

The fundamentals of PUEA is that the adversary is not focused on jamming primary users, but on forestalling idle spectrum bands that could have been used by other secondary users. Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack.

A selfish PUE attacker aims to prevent other secondary users from competing for that band by sending signals with similar characteristics to those of the primary user, whereas the malicious user launching an attack in the same manner is more interested in obstructing the whole dynamic spectrum access process rather than monopolizing the utilization of the frequency spectrum resource.

Depending on the motivation behind the attack, a PUE attack can be classified as either a greedy PUE attack or a malicious PUE attack:

- Greedy nodes that by transmitting fake incumbent signals force all other users to vacate a specific band (spectrum hole) in order to acquire its exclusive use.

- Malicious nodes (adversaries) that mimic incumbent signals in order to cause Denial of Service (DoS) attacks.

  Malicious nodes can cooperate and transmit fake incumbent signals in more than one band, thus causing extensive DoS attacks making a CRN hop from band to band, severely disrupting its operation.

  Furthermore, adversaries could also cause DoS attacks to PU networks by creating harmful interference.[5]

Considering different adversaries, assumptions whether the location of users are known, whether cooperating schemes between SUs are used or not, and if FCC's mandate that no modification to

incumbent signal is necessary has been followed, several PUEA combating techniques have been proposed (and tested) in the literature:

- Chen et al. [13] – a transmitter verification scheme - called LocDef (localization based defense) - is proposed, which verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics.

  To estimate the location of the signal transmitter, LocDef employs a non-interactive localization scheme.

  This approach consists of three phases: (i) verification of signal characteristics, (ii) received signal energy estimation, and (iii) localization of the transmitter. It mainly focuses on the localization of the transmitter using a method based on RSS measurements collected by a wireless sensor network.

  Based on the distribution of the RSS values, a decision is made about if the transmitter is an incumbent transmitter or an attacker.

  Here, the location of the incumbent transmitter has to be known a priori.

  However, the proposed method has several limitations, such as the use of RSS (which can have large fluctuations); the assumption of using fixed transmission power (not taking sophisticated adversaries into account) and the need for the location of the incumbent transmitter to be known a priori.

- Jin et al. [14] - present an analytical model as well as a practical mechanism to detect PUEAs without using any location information.

  An analysis using Fenton's approximation and Wald's sequential probability ratio test (WSPRT) to detect PUEA is given.

  The detection mechanism allows the user to set thresholds on probability of missing the primary user and the probability of successful PUEA and hence can accommodate a range of sensitivities.

  It is possible to construct tests that always keep the probability of missing the primary user below a specified threshold, while still keeping the probability of successful PUEA low.

  Mathematical expressions are derived for the computation of: (i) the Probability Density Function (PDF) of the received power to a SU due to a PU, and (ii) the PDF of the received power to a SU due to malicious users.

  Then, WSPRT is used to make a decision between two hypotheses (H0: primary transmitter, H1: malicious user).

In [15] same authors compare the results produced by WSPRT with those produced by using Neyman-Pearson Composite Hypothesis Testing (NPCHT), also taking into account multiple malicious users, as well as the fading characteristics of the wireless environments.

According to their simulations, WSPRT achieves a 50% better efficiency in terms of detecting PUEA.

- Chen et al. [16] - authors characterize an advanced primary user emulation attack and an advanced countermeasure against such an attack.

  Specifically, they show that both the attacker and the defender can apply estimation techniques and learning methods to obtain the key information of the environment and thus design better strategies.

  They further demonstrate that the advanced attack strategy can defeat the naive defense technique that focuses only on the received signal power, whereas the advanced defense strategy that exploits the invariant of communication channels can counteract the advanced attack effectively.

  A key observation stated by the authors and used in this method is that an attacker can mimic many characteristics of a PU signal, but it cannot easily emulate the feature of the communication channel.

  SUs perform energy detection as this method, according to the authors, has three advantages: (i) it is easily implemented, (ii) a sophisticated attacker can emulate several characteristics of the primary signal such as cyclostationary characteristics and modulation; thus it would be more difficult for a SU to detect the attack when using the matched filter or the cyclostationary spectrum sensing approaches, and (iii) the method proposed here can be extended for the other spectrum sensing methods.

- Liu et al. [21] - authors propose a novel approach for authenticating primary users' signals in CRNs, which conforms to FCC's requirement.

  This approach integrates cryptographic signatures and wireless link signatures (derived from physical radio channel characteristics) to enable primary user detection in the presence of attackers.

  Essential to the approach is a helper node placed physically close to a primary user. The helper node serves as a "bridge" to enable a secondary user to verify cryptographic signatures carried by the helper node's signals and then obtain the helper node's authentic link signatures to verify the primary user's signals.

  A key contribution is a novel physical layer authentication technique that enables the helper node to authenticate signals from its associated primary user.

Authors state that, unlike previous techniques for link signatures, their approach explores the geographical proximity of the helper node to the primary user, and thus does not require any training process.

The authors also demonstrate a real implementation of the proposed approach using GNU radios and verify some of their simulation results.

3.1.1.2.2 Spectrum Sensing Data Falsification Attacks

Several transmission features such as signal fading, multi-path, etc., can cause the received signal power to be lower of what path loss models have predicted. This leads to undetected primary signals and harmful interference to PUs.

There are two types of fading: shadow fading that is frequency independent, and multi-path fading that is frequency dependent.

Shadow fading can cause the “hidden node” problem where a SU, although located within the transmission range of a primary network, fails to detect primary transmissions.

SU1 fails to detect the transmission of incumbent signals because of shadow fading, so it accesses the incumbent frequency band causing harmful interference to PU1.

A solution to this problem is the collaborative spectrum sensing technique, where a number of users sense the environment and send their observations to a fusion center (FC).

FC then fuses the provided information taking the final decision regarding the presence or absence of incumbent transmissions.

Another type of sensing is the collaborative distributed sensing where no FC is used. In this case, each SU makes its decision based not only on its observations but also on observations shared by other SUs.

For both types of collaboration, distributed or centralized, SUs have to share their observations or transmit them to a FC.

There is always the possibility that one or more SUs send false observations, intentionally or unintentionally. Similarly to PUEAs, nodes sending false observations can be categorized as follows:

- Malicious users that send false observations in order to confuse other nodes or the FC. They aim to lead FC or the rest of the nodes to falsely conclude that there is an ongoing incumbent transmission where there isn’t, or make them believe that there are no incumbent transmissions when there are.

  In the first case, the legitimate SUs will evacuate the specific band, while in the second case they will cause harmful interference to the PUs.

- Greedy users that continuously report that a specific spectrum hole is occupied by incumbent signals. The goal of these users is to monopolize the specific band by forcing all other nodes to evacuate it.

- Unintentionally misbehaving users that report faulty observations for spectrum availability, not because they are malicious or greedy, but because parts of their software or hardware are malfunctioning. The reason for this can be a random fault or a virus.

Regardless of the type of the misbehaving users, the reliability of collaborative spectrum sensing can be severely degraded by faulty provided observations.

This is called as Spectrum Sensing Data Falsification (SSDF) attack. FC receives observations from SUs and then it decides about the presence or absence of primary transmissions.

This type of cooperation can be exploited by malicious users that send malicious reports to the FC on purpose.[5]

Some of the contributions for the detection of SSDF attacks – mutually differentiated by type of reporting (binary vs. continuous), fusion rules used (AND-rule; OR-rule; average-rule; Dempster-Shafer etc.) are:

- Wang et al. [18] – develop a malicious user detection algorithm that calculates the suspicious level of secondary users based on their past reports.

  Then, the trust values as well as consistency values are calculated and are used to eliminate the malicious users' influence on the primary user detection results.

  Through simulations, it was shown that even a single malicious user can significantly degrade the performance of collaborative sensing.

  The proposed trust value indicator can effectively differentiate honest and malicious secondary users.

  For the evaluation of this scheme the authors compare their approach using different fusion rules (OR, K2).

  They also show how their approach can increase the detection probability and decrease the false alarm rate significantly when the OR rule is used compared to an attack-oblivious method. However, only one adversary has been considered.

- Rawal et al. [19] - The authors propose a method to identify attackers by counting mismatches between their local decisions and the global decision at the FC over a time window and then remove them from the data fusion process.

  Hence, for the computation of the reputation metric the output of each SU is compared to the decision made by the FC.

  If there is a decision mismatch, the reputation metric of the corresponding user increases by one. The smaller the reputation metric is, the more reliable the user is.

  If the reputation metric of a user exceeds a predefined threshold, its decisions are isolated and thus not used by the FC.

This work is somewhat similar to, [18], but the key difference is that the reputation metric is restored in case a node temporarily misbehaves.

- Noon et al. [20] - a hit-and-run attack policy is proposed, which cannot be mitigated by traditional approaches of attacker detection in cognitive radio systems.

  Motivated by the system of points for penalizing reckless drivers in DMV, a point based attacker detection algorithm is proposed, whose effectiveness is demonstrated by numerical simulations.

  The adversary is an intelligent attacker that, by knowing the fusion technique used by the FC, deviates between an honest mode and a lying mode.

  The attacker estimates its own suspicious level and as long as it is below a threshold h, it reports faulty observations (lying mode). If its suspicious level drops below a threshold, it behaves legitimately again (honest mode).

  The detection scheme functions in a way that when the suspicious level of a node becomes larger than h, a point is assigned to this user.

  When it exceeds a predefined threshold, the observations of this user are ignored permanently. A drawback of this method is that a user is permanently removed from a CRN if it collects enough points.

- Kaligineedi et al. [21] - authors have devised schemes to identify and nullify the effect of malicious nodes for the case where energy detectors are used by the sensing devices.

  A simple and fast average combination that's using a pre-filtering phase based on quartiles is presented.
  Then, a trust factor is computed over a sample period that identifies more outliers. Using simulations, it was verified that the proposed schemes can identify 'Always Yes' users, 'Always No' users and malicious nodes producing extreme values.

- Min et al. [22] – an attack-tolerant distributed sensing protocol (ADSP) is proposed, under which sensors in close proximity are grouped into a cluster, and sensors in a cluster cooperatively safeguard distributed sensing.

  The heart of ADSP is a novel shadow fading correlation-based filter tailored to anomaly detection, by which the fusion center pre-filters abnormal sensor reports via cross-validation.

  By realizing this correlation filter, ADSP minimizes the impact of an attack on the performance of distributed sensing, while incurring minimal processing and communications overheads. This approach consists of two phases.

First, pre-filtering takes place where possible outliers are isolated and the information they provide is ignored by the FC.

During this phase, a per-sample abnormal behavior is detected by examining similarities using the Conditional Probability Density Function (CPDF) of the power for the sensors belonging to the same cluster report.

If CPDF lies between two defined thresholds, the SU is characterized as legitimate, otherwise it is tagged as an outlier and its reports are ignored.

As the authors note, this pre-filtering step is not adequate in very low SNR environments due to the high sensitivity of the fusion decision to RSS values.

For this reason, a second line of defense follows where a weighted gain combining method assigns weights to the outputs of the sensors based on their CPDF.

The FC accumulates the reports sent by all sensors (excluding the users identified as outliers in the pre-filtering phase) and if the total output exceeds a threshold, the frequency band under examination is marked as busy, otherwise it is marked as vacant.

3.1.1.2.3 Spectrum Sensing Data Falsification Attacks

In some approaches, a dedicated channel is used to exchange sensing information:

- between the base station and the secondary users if the CRN is centralized (i.e. DIMSUMnet)

and

- between secondary users if it is distributed (such as KNOWS or CORVUS)

A malicious user could jam this channel, disrupting all transmissions and preventing elements within the CRN from sharing information about spectrum usage.

The lack of knowledge about available bands keeps the CRN from operating (DoS attack). Moreover, eavesdropping on the control data provides the attacker with all the required information to detect which new channel the CRN is switching to.

The need of securing the common control data is hence patently obvious. 802.22 Working Group is aware of this threat and has proposed mechanisms to protect such information.

We consider that the impact of this attack is more relevant in centralized CRNs as an attacker can focus on jamming the control channel within the base station vicinity (single point of failure) and thus easily affecting the whole network.

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

- MAC spoofing, where attackers send spurious messages aiming to disrupt the operation of CRN (e.g. channel negotiation).

  Multi-hop CRNs are more vulnerable to this type of attack as there is no central entity to control the authentication between the nodes and protect data integrity.

- Congestion attacks, where attackers flood CCC in order to cause an extended DoS attack.

- Jamming attacks, where attackers cause DoS attacks at the physical layer by creating interference.

Some of the contributions dealing with the attacks targeting the CCC are:

- Bian et al. [23] – the authors show how DoS attacks using spurious MAC frames affect the performance of a multi-hop CRN.
  The degree of degradation is heavily affected by the number of the attackers.

  The same work studies the effect on network performance when nodes act selfishly. In a multi-hop CRN, selfish nodes that are located along the path of normal-behaved nodes can drop their packets; thus monopolizing the medium.

- Safdar et al. [24] – the authors present a novel framework for providing common control channel security for co-operatively communicating cognitive radio nodes.

  It is investigated how two cognitive radio nodes can authenticate each other prior to any confidential channel negotiations to ensure subsequent security against attacks.

3.1.1.2.4 Beacon Falsification Attacks

Beacon Falsification (BF) attacks is the set of attacks specifically targeting the MAC layers within the IEEE 802.22-based networks.

The attacks consist of disrupting the exclusive spectrum sharing by transmission of spurious beacons that contain very large CCN values by an adversary.

To counter BF attacks, Bian et al. in [20] propose an inter-cell key management scheme.

3.1.1.2.5 Cross-layer Attacks

“Cross-layer” attacks refer to attacks that target multiple layers of the CRNs, and can affect the whole cognitive cycle, as attacks at all layers become feasible.

Small Backoff Window (SBW) is a very common attack in wireless networks where malicious users choose a very small value for minimum Contention Window (CWmin) aiming to monopolize bandwidth. SBW attacks are feasible against CRs with MAC layers using a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) type of access.

Wang et al. in [25] study specific attack, time domain coordination of RFSD and SBW. A cross-layer trust defense scheme was designed by developing (1) abnormal detection schemes in PHY and MAC layers and (2) the cross-layer trust manager.

The simulations showed how this scheme fates against this specific cross-layer attack.

The Lion attack is defined as a jamming targeted to reduce the throughput of TCP by forcing frequency handoffs.

The handoff process involves sensing the medium looking for vacant channels and choosing the best one according to some criteria, thus incurring high latencies until the transmission is resumed.

A malicious user trying to disrupt a TCP connection of a secondary user can perform a PUEA to force a handoff in the CRN.

As the transport layer is not aware of the disconnection, it keeps sending data segments which are queued at lower layers but not transmitted and thus TCP segments can be delayed or even lost.

As the TCP sender is allowed to transmit new data upon reception of acknowledgments, loss or delay of segments can lead to a period of inactivity of the former.

Hernandez-Serrano et al. in [26] evaluate the impact of the Lion attack on TCP performance through an analytical model.

The model provides an expression for the average time of inactivity of a TCP sender due to the attack and also the percentage of inactivity, parameters which measure the impact of the attack on TCP throughput.

However, for mitigating the attack, only general recommendations are given, such as: making TCP layer aware of the cognitive capability of CRs so it acquires information from the physical layer, and securing the operation of a CCC for channel negotiations during the attack.

3.1.1.3 Cognitive Radio Node Simulator

In pSHIELD began the implementation of a Cognitive Radio Node that is able to receive radio parameters from moving hosts and automatically detect possible threats.

The Hardware and the Software of this platform will evolve during nSHIELD project, first adopting a smaller and more powerful HW that can support the evolution of the cognitive algorithms, allowing the studies and the experimentations of new concepts and features.

The internal architecture of the Node is able to learn typical safe environment features, thus detecting the presence of external attackers by analyzing 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 the 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 with the agent itself. In this way the node can update its radio information in order to use the radio resources efficiently and securely.

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

From the configuration database, the node knows which frequencies are being used by which agent, as well as which ones are free to use.

If the new agent enters the scene whilst the communication is ongoing, the cognitive node senses the radio parameters of the agent and is able to modify and adapt agents' radio parameters when necessary.

In the presence of the jammer at specific frequency in a cluster, the cognitive node sends the 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, both with active communication on different frequencies.

Areas affected by the movement of such entities are three jammers that inhibit different frequencies and present a range of different from each other.

Moving agents in the scene and the presence of jammers are dynamically created through the dedicated simulator.

The simulator sends to the cognitive node the positioning data, namely the trajectories of the agents (like a tracker) and radio data describing 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 regarding the quality of communication.

Figure 3: Simulator - considered scene (Jammer, First Agent and Second Agent in the scene)

In the simulator there are six types of interaction considered between two different agents (guard/intruder), namely:

a) 'Agents in Motion': Two entities with communication capabilities moving in the scene without interacting with 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 is the guard and the other is the intruder.

When the guard spots the intruder inside the region under its control, it starts the procedures to identify and localize the menace in order to counteract the action of the intruder whereas the intruder tries to overcome the countermeasures quickly.

c) 'Meeting Agents': Two communication entities meet/gather inside the scene and after meeting they link together.

d) 'Leave & Meet Agents': Two communication entities link inside the scene and leave the area individually.

e) 'Running Agents': Two communication entities running inside the scene but without interacting with each other.

f) 'Run & Walk Agents': One is running inside the area under consideration and the other is walking but without interacting with each other.

In order to give an idea of what will be tested through the mentioned mixed HW-platform+simulator environment, the following is an example about a concept that was identified and preliminary verified in pSHIELD and that will be exploited in nSHIELD.

These tests will demonstrate the value added by the Smart Transmission Networks to the SPD functionalities, compared with the traditional behavior of a Cognitive Radio Node:

A node that would like to belong to the nSHIELD SPD network first must transmit its GPS position. All the nodes continuously measure and transmit the value of the strengths of the radio signals (RSS) they're receiving.

Each SPD node has the ability to fuse the data received from the other nodes, so, comparing the new 'guest' position declaration with the RSS of the other trusted nodes, together with their position, it can decide if this guest may be 'malicious'.

3.1.1.4 Reputation in network layer – Mechanisms

There are many reputation mechanisms that have been deployed across network layer; the following section describes some of them:

Reputation for ad-hoc networks[1]: Ad-hoc networks are intrinsically dynamic and thus many unexpected elements can be added dynamically putting in risk the purpose of the network.

The purpose of this work is to provide a mechanism for detecting malicious incorrect packet forwarding attacks.

To this end, a trust model extending routing protocols and based on the reputation concept is developed the model provides two main functionalities: monitoring the behaviour of the neighboring nodes in the network and computing their reputations based on the information provided by the monitoring.

Selfish nodes isolation[2]: This mechanism provides a distributed reputation evaluation scheme implemented autonomously at every node in an ad hoc network with the objective of identifying and isolating selfish neighbours.

Each node maintains a reputation table, where a reputation index is stored for each of the node's immediate neighbours.

This protocol provides routing protocol independence, no communication overhead, directional transmission and elimination of an overlay trust management (this just on of the main difference compared to nSHIELD overlay layer which will compose trust)

[1] Yacine Rebahi, Vicente .E Mujica-V, Dorgham Sisalem Fraunhofer Fokus, Kaiserin Augusta Allee 31, 10589, Germany, 2004

[2] A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks, M. Tamer Refaei, Vivek Srivastava, Luiz DaSilva, Mohamed Eltoweissy, 2005

Reputation for wireless networks[3]: this work encompasses several algorithms brought from the game theory.

It uses the game theory itself (prisoner dilemma), strategies and pay-off and Nash equilibrium in order to develop reputation based techniques. Theses are usually very interesting for many elements.

3.1.1.4.1 Main Attacks in Reputation-based network layer

Reputation based techniques enable some new interaction with different and normally external network elements. This causes new risk that must be detected. The following attacks are the main risks that could be exploited:

Spoofing: it could happen that one person or software might attack the ARP table on Ethernet layer. The aim is to associate attacker's MAC address with the IP address of another host, so that there is a masquerade action.

This would let the attacker to intercept data frames and act as an opening for other malicious attacks such as DoS or man in the middle.

There are 3 main safeguards related to Spoofing attack: mapping statically MAC and IP addresses, which it makes more complex its management, deploying ad-hoc ARP spoofing detection software and/or being helped by the OS security.

ID Stealth: This is a variant of the spoofing attack. One attacker might take advantage of the reputation of one element in the network if its ID is stolen. This is an opening for further malicious attacks the hacker may perform. ID steals happen if a *man in the middle* occurs and it might cause a great impact.

Shilling: although this attack is oriented to peer-to-peer networks, it might also happen in embedded networks.

This is about making a resource more valuable that it really is. It starts when multiple elements or instances give value to one particular resource in the network.

This element will acquire a virtual reputation and therefore present a better curriculum although it might happen that it is vulnerable.

The other elements of the network will interact with this revaluated element and consequently will put on risk themselves.

Shilling is a social attack and is very interesting for analsying the network elements behavior according to reputation.

As countermeasure, systems should analyse how rapid one element should acquire a good reputation. This is so because rapid reputation acquisition often implies risk.

3.1.1.4.2 Reputation in nSHIELD

nSHIELD will use reputation based techniques.

This will be based on the parameter of level agreements that systems and elements will expose as interface to external environment.

These parameters, in turn, will be based on metrics that will are define in deliverable 2.5.

---

3 Performance Analysis of Reputation-based Mechanisms for Multi-hop Wireless Networks, Fabio Milan Dipartimento di Elettronica Politecnico di Torino Turin, Italy, Juan Jos´e Jaramillo and R. Srikant Coordinated Science Laboratory Dept. of Electrical and Computer Engineering University of Illinois at Urbana-Champaign

3.1.1.5 Intrusion Detection Systems in WSN

A WSN is a network compounded by small embedded systems that gather information from its sensor, make a set of computations and communicate via wireless links with other nodes. These nodes can be deployed in many environments and each environment has its own needs. For example, in hostile ones WSN need to be secure and trustworthy, while in unattended environments they need to be autonomous and self-sufficient. Due to these reasons the complexity of sensors may vary significantly, from small computation power with low energy consumption to large nodes with complex systems used in military environments. But in most cases nodes are designed as simple as possible to minimize production costs and reduce power consumption.

Because nodes are often responsible for managing critical systems, security becomes one of the most important features in WSN. In hostile environments an adversary can manage to compromise one or more nodes, and the security systems have to minimize the damage. Prevention methods like encryption and authentication can reduce intrusions but not eliminate them. These methods cannot defend the system from compromised nodes that are already part of the network and thus use proper private keys. Security research assumes that weak links, which can be exploited, can always exist in the network, no matter how many intrusion prevention policies are established. The undetected weak links provide the attackers a point to provoke network failures. If a system is able to detect the intruder soon enough, appropriate measures can be taken before any damage is done or any data is compromised. In this area, intrusion detection systems are responsible for detecting a possible attack and minimizing the risks.

Due to these reasons an IDS for WSNs needs to have some specific characteristics, and some of these specifications that an IDS should have are the following:

- The IDS should not introduce a new weakness in the WSN.
- The IDS should run continuously and remain transparent to the system and users.
- The IDS agents cannot consume so much bandwidth and resources from the node.
- It must be fault tolerant and be able to recover from system failures.
- It must be able to respond to attacks without human intervention.

During the last few years, some works have been published where intrusion detection systems were applied in WSN environments [27] [28] [29]. Most of these studies have covered the local detection problem, where nodes detect specific attacks that happen in their network.

A description of the requirements of a WSN oriented IDS is given in [30]. Embedded systems, by definition, must use the minimum resources possible to preserve their lifetime. One of the main characteristic is that it must work with only localized and partial data due to the possible lack of centralized points with a global view. Other characteristics are that the system can never trust any node completely and that the system should be fully distributed. Finally, it should be able to withstand an attack to the IDS itself.

Similar IDS are proposed in [28] and [31], where there are special purpose nodes in the network which are responsible for monitoring other nodes. They listen to messages in their same radio range and store message fields that can be useful to an IDS running in a sensor node. There are some other different points of view in the design of IDS in WSN, for example [32], where nodes are selfish and try to preserve their resources at expense of others. Other works,[33] and [34], keep the idea of no collaboration among sensor nodes and assume that the ad hoc network routing protocols can be applied to WSN.

A distributed intelligent agent-based system is proposed in [35]. It detects intrusions in a fully distributed way. This characteristic comes from the fact that all nodes have an independent IDS agent installed. This agent is able to detect intrusions locally, always based on data collected by the same node and by neighbour nodes. Once an intrusion is detected, the responses or actions taken to isolate it are based on a decision that is made collaboratively by the set of participating nodes. Other collaborative approaches on the local detection of selective forwarding and sinkhole attacks can be found in [36] and [37] .

Intrusion detection in ad-hoc networks has had more attention as described in [38] . Distributed and collaborative IDS architectures are preferable for these networks. This way, detailed distributed designs, actual detection techniques and system performance have been more deeply studied. It must be taken into account that wireless sensor networks compared to ad-hoc networks are generally much more resource constrained. Approaches to a more sensor collaborative system rather than a specific attacks detection system can be found in [27].

Regarding distributed systems, LIDeA is a lightweight WSN oriented IDS [39] . It is based on a distributed architecture, where nodes listen to their neighbour nodes and collaborate with each other in order to detect an intrusion successfully. LIDeA, uses components and interfaces of TinyOS [40], a free and open source component-based operating system and WSN oriented platform.

Another distributed IDS is presented in [41]. In this work a misuse-based combined with anomaly-based IDS in a two level distributed hierarchy is proposed. There are two main parts in this IDS: The IDS Central Agent, which is in charge of recognizing attacks by exploiting control data and alarms sent by Local Agents (LA), and the IDS Local Agent which is located in each node. This LA is compound by other three parts, the Local Packet Monitor (it is in charge of analysing the traffic flowing through the node), the Control Data Collector (gathers measures to be sent to the IDS Central Agent) and the Local Detection Engine (it is in charge of detecting suspicious activities and rising alerts, receiving responses from the Central Agent and performing possible recovery actions). The usage of an anomaly-based approach for local detection might result in a high number of false positives. The usage of temporary local decisions allows the mitigation of such sided effect and especially avoids the triggering of responses for intermittent anomalies. The temporary decisions made by the Local Agent may be made persistent by the Central Agent. The Central Agent detects attacks based on known patterns of attack features (misuse-based detection), and when it makes its final decision, the base station propagates the decision to the Local Agents for its enforcement.

Finally a Hybrid Intrusion Detection System (HIDS + NIDS) has been proposed in [42]. This system is based on a hybrid star architecture and applied to Cluster Wireless Sensor Networks (CWSN) where intrusions are detected by Cluster Heads. The proposed IDS consists of an anomaly detection and misuse detection model. It filters a large number of packet records, using the anomaly detection model, and performs a second detection with the misuse detection model, when the packet can be determined as an intrusion. Therefore, it efficiently detects intrusions and avoids the resource waste. Finally, integrates the outputs of the anomaly detection and misuse detection models with a decision making model. This determines the presence of an intrusion, and classifies the type of the attack. The output of the decision making model is then reported to an administrator for follow-up work. This method not only decreases the threat of having successful attacks in the system, but also helps the user handle and correct the system further with hybrid detection.

A similar Hybrid IDS is presented in [43], where the system is based in anomaly and misuse techniques. The attacks are detected through the collaboration of global and local agents integrated in the application layer of nodes. A defense method and four algorithms to detect and isolate malicious nodes are also proposed.

3.1.1.6 Reputation and Trust-based IDS in WSN

In recent years a growing number of studies have been conducted on the use of reputation systems in sensor and adhoc networks [19]. But only RFSN [20] and DRBTS [21] have focused on the use of reputation systems in WSN.

DRBTS stands for “Distributed Reputation and trust-based Beacon Trust System”. This model makes use of some special nodes called Beacon Nodes (BN) that can monitor each node around and report to the

rest of the network of gathered information. This data is gathered using watchdog mechanism, this mechanism is used assiduously in WSNs and is explained in [22].

Meanwhile RFSN or Reputation-based Framework for Sensor Network is a design based on the watchdog mechanism as well, but this design keeps this mechanism in each node of the network. Making use of this, a node can classify each action as a cooperative or non-cooperative creating the reputation of the nodes around.

4 References

[1] V. Drakulovski et al “System Requirements and Specification for the pSHIELD-project”, http://www.pshield.eu/index.php?option=com_docman&task=doc_download&gid=238&Itemid=37

[2] M. Al-Kuwaiti, N. Kyriakopoulos, S. Hussein, A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability, IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second Quarter 2009.

[3] James McCabe, Practical Computer Network Analysis and Design, Morgan Kaufmann Publishers, Inc., CA, 1998, pp. 1-9.

[4] pSHIELD project, Deliverables D2.1.1, “Preliminary SPD Metrics Specification for the pSHIELD project,” September 2011.

[5] A. G. Fragkiadakis, E. Z. Tragos, I. G. Askoxylakis, “A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks”, Communications Surveys & Tutorials, IEEE, 2012, pp. 1-18

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

[7] H. Uchikawa, K. Umebayashi, and R. Kohno, “Secure download system based on software defined radio composed of FPGAs,” in PIMRC, 2002, pp. 437–441.

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

[9] C. Li, A. Raghunathan, and N. Jha, “An architecture for secure software defined radio,” in Proc. Date ’09, 2009, pp. 448–453.

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

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

[12] D. S. Dawoud, “A Proposal for Secure Software Download in SDR”, IEEE Africon, 2004

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

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

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

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

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

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

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

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

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

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

[23] K. Bian and J. Park, “MAC-layer misbehaviours in multi-hop cognitive radio networks,” in Proc. UKC, 2006, pp. 1–8.

[24] K. Bian and J. Park, “Security vulnerabilities in IEEE 802.22,” in Proc. WICON, 2008, pp. 1–9.

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

[26] J. Hernandez-Serrano, O. Leon, and M. Soriano, “Modelling the lion attack in cognitive radio networks,” EURASIP Journal on Wireless Communications and Networking, vol. 2011, p. 10 pages, 2011.

[27] I. Krontiris, Z. Benenson, T. Giannetsos, F. Freiling and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks," Wireless Sensor Networks, pp. 263-278, 2009.

[28] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, 2005, pp. 16-23.

[29] P. Techateerawat and A. Jennings, "Energy efficiency of intrusion detection systems in wireless sensor networks," in Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2006, pp. 227-230.

[30] A. STETSKO, "INTRUSION DETECTION FOR WIRELESS SENSOR NETWORKS," .

[31] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Wireless and Mobile Computing, Networking and Communications, 2005.(WiMob'2005), IEEE International Conference on, 2005, pp. 253-259 Vol. 3.

[32] F. Kargl, A. Klenk, M. Weber and S. Schlott, "Sensors for detection of misbehaving nodes in MANETs," in Detection of Intrusions and Malware & Vulnerability Assessment, GI SIG SIDAR Workshop, DIMVA, 2004, pp. 83-97.

[33]] L. Chong Eik, N. Mun Yong, L. Christopher and P. Marimuthu, "Intrusion Detection for Routing Attacks in Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2, pp. 313-332, 1900.

[34] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," Journal of High Speed Networks, vol. 15, pp. 33-51, 2006.

[35] A. Giannetsos, "Intrusion detection in wireless sensor networks," 2009.

[36] K. Ioannis, T. Dimitriou and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proceedings of the 13th European Wireless Conference, 2007, .

[37] I. Krontiris, T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," Algorithmic Aspects of Wireless Sensor Networks, pp. 150-161, 2008.

[38] A. Mishra, K. Nadkarni and A. Patcha, "Intrusion detection in wireless ad hoc networks," Wireless Communications, IEEE, vol. 11, pp. 48-60, 2004.

[39] I. Krontiris, T. Giannetsos and T. Dimitriou, "LIDeA: A distributed lightweight intrusion detection architecture for sensor networks," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1-10.

[40] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh and E. Brewer, "TinyOS: An operating system for sensor networks," Ambient Intelligence, vol. 35, 2005.

[41] L. Coppolino, S. D'Antonio, L. Romano and G. Spagnuolo, "An intrusion detection system for critical information infrastructures using wireless sensor network technologies," in Critical Infrastructure (CRIS), 2010 5th International Conference on, pp. 1-8.

[42] K. Yan, S. Wang and C. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks," Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, pp. 18-20, 2009.

[43] T. H. Hai, F. Khan and E. N. Huh, "Hybrid intrusion detection system for wireless sensor networks," in Proceedings of the 2007 International Conference on Computational Science and its Applications-Volume Part II, 2007, pp. 383-396.

[44] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, “Reputation and trust-based systems for ad hoc and sensor networks,” Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2006.

[45] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, “Reputation-based framework for high integrity sensor networks,” ACM Transactions on Sensor Networks (TOSN), vol. 4, no. 3, p. 15, 2008.

[46] A. Srinivasan, J. Teitelbaum, and J. Wu, “Drbts: Distributed reputationbased beacon trust system,” in Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on. IEEE, 2006, pp. 277–283.

[47] L. Huang and L. Liu, “Extended watchdog mechanism for wireless sensor networks,” Journal of Information and Computing Science, vol. 3, no. 1, pp. 39–48, 2008.